Cryptographie à l'ère quantique

Séminaire DSI, Eybens, juin 2026

Léo Colisson Palais
leo.colisson-palais@univ-grenoble-alpes.fr

Université Grenoble Alpes

Les étranges lois de la physique quantique

Cosmic Eye

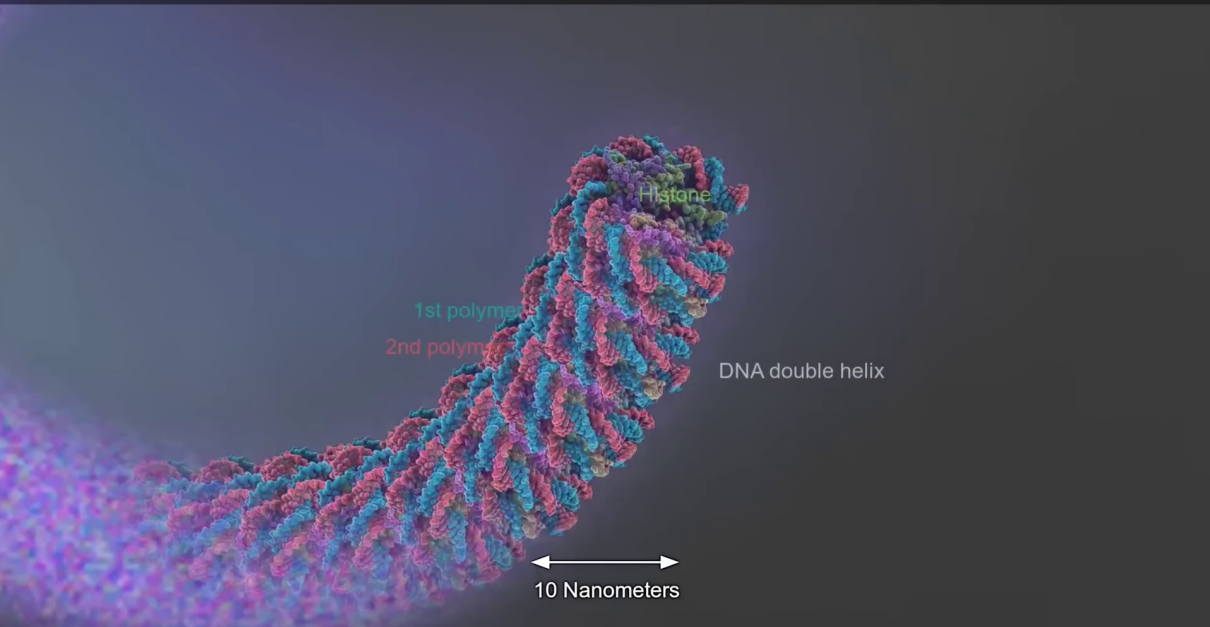
a state-of-the-art view of the universe

version 2.0

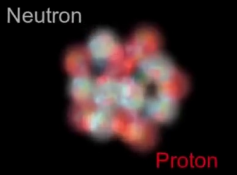
Danail Obreschkow

Smiling Face

10-nm Fiber


Histone
1st polymer
2nd polymer
DNA double helix
10 Nanometers

Protons and Neutrons



10 Femtometers

Les étranges lois du monde quantique

Les étranges lois du monde quantique

Les étranges lois du monde quantique

Les étranges lois du monde quantique

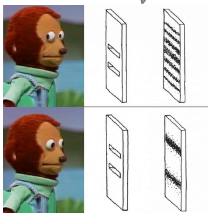
Observer un objet le modifie/détruit !

Les étranges lois du monde quantique

Les étranges lois du monde quantique

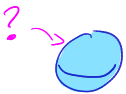
Les étranges lois du monde quantique

Observer un objet le modifie/détruit !



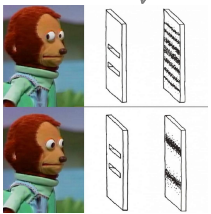
cf fentes de young

Copier / coller ... Impossible !



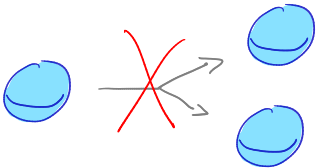
Les étranges lois du monde quantique

Observer un objet le modifie/détruit.



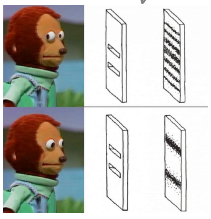
cf fentes de young

Copier/coller... Impossible !

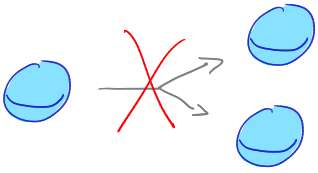


Les étranges lois du monde quantique

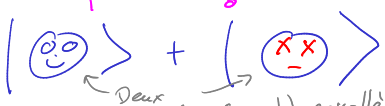
Observer un objet le modifie/détruit.



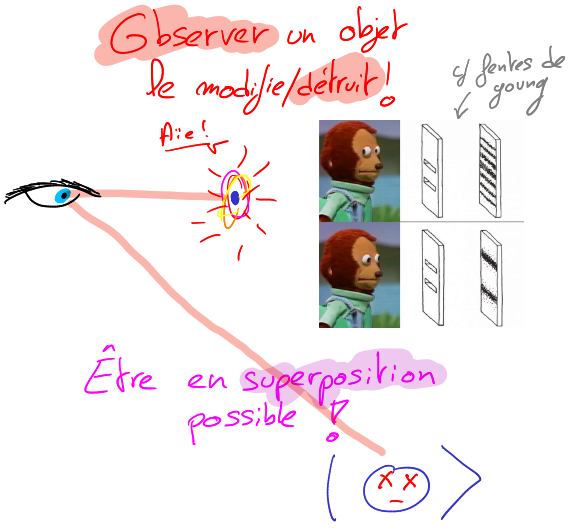
Copier / coller... Impossible !

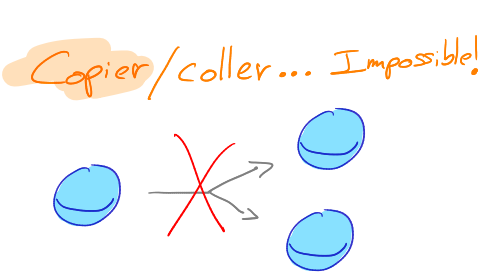


Être en superposition possible ?

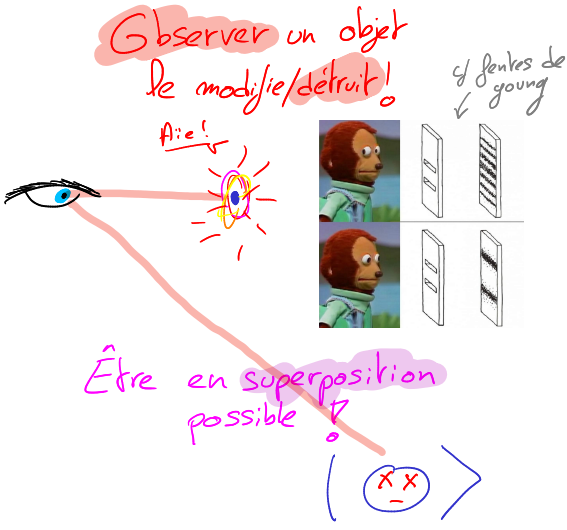


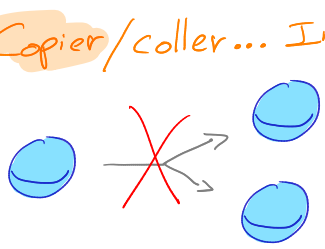
Les étranges lois du monde quantique

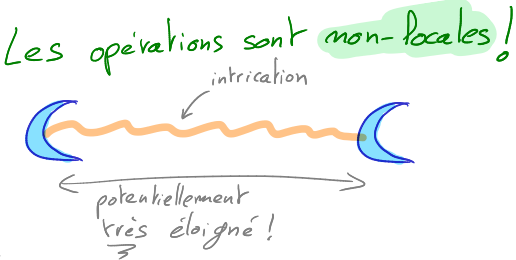




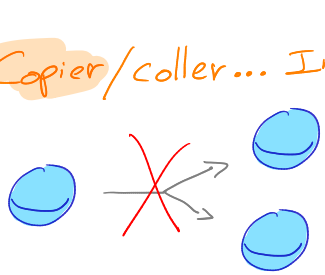
Les étranges lois du monde quantique

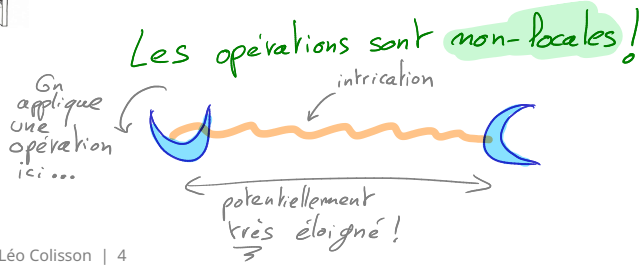






Les étranges lois du monde quantique

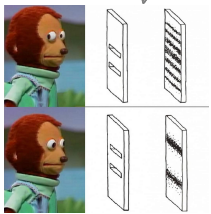




Les étranges lois du monde quantique

Observer un objet le modifie/détruit !

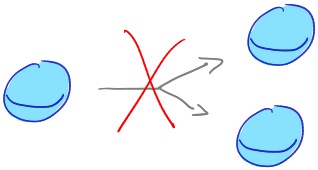
cf fentes de young



Aïe !

Être en superposition possible ?

Copier / coller ... Impossible !



Les opérations sont non-locales !

On applique une opération ici ...

intrication

... une opération est instantanément appliquée de l'autre côté !

potentiellement très éloigné !

Quantique : les modifications sont non-locales

Attention !!!

Même si l'état est modifié instantanément, il est toujours

impossible de communiquer plus vite que la vitesse de la lumière !

https://drgoulu.com

L’informatique quantique

Qubits

Qubits

Made from infinitesimally small particles:

Qubits

Made from infinitesimally small particles:

E.g.:
- photons

Qubits

Made from infinitesimally small particles:

E.g.:
- photons
- cold atoms
- ...

Qubits

Qubits

Qubits

0

Qubits

Qubits

Qubits

Superposition

$$a_0 |0\rangle + a_1 |1\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

Qubits

Superposition

$$a_0 |0\rangle + a_1 |1\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

$$|+_\theta\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta} |1\rangle)$$

Qubit

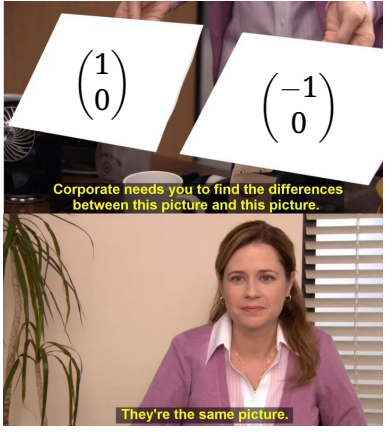
Qubit

Un qubit est un vecteur $|\psi\rangle := \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^2$ de norme 1, i.e. $|a|^2 + |b|^2 = 1$.

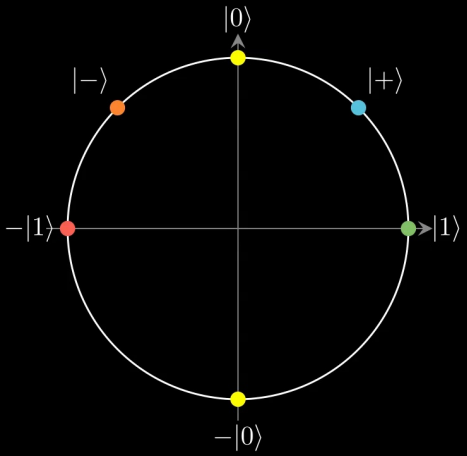
On note $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Qubits

La **phase globale** d'un état n'est PAS physiquement observable !

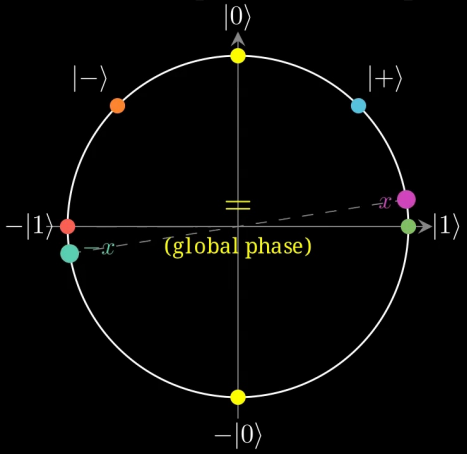


Explaination of the bloch sphere

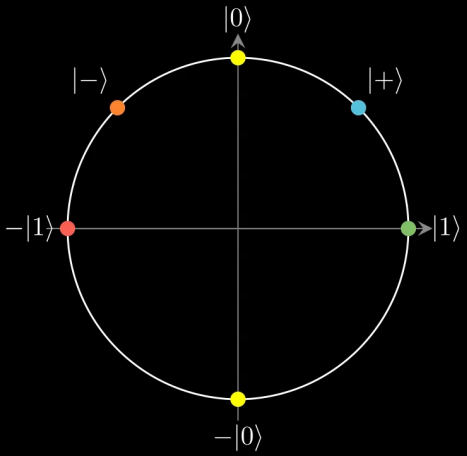


Explaination of the bloch sphere

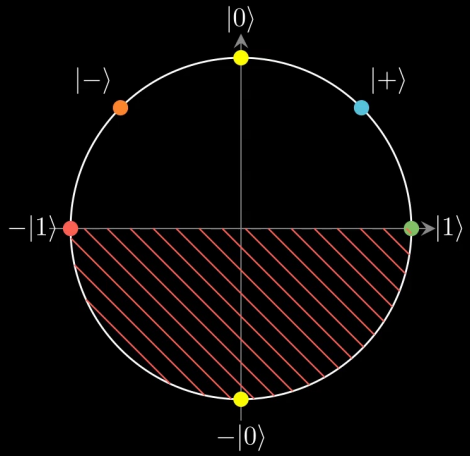
x and its antipodal −x are equal



Explaination of the bloch sphere

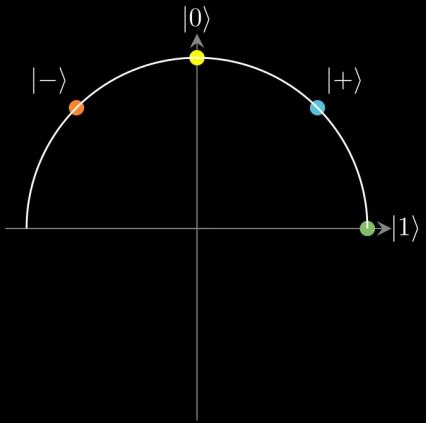


Explaination of the bloch sphere

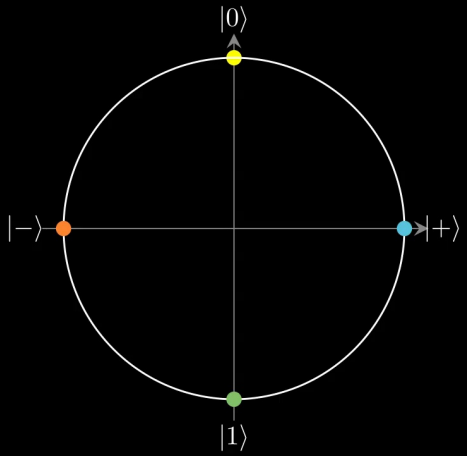


Bottom half is redundant $(e^{i\varphi}|\psi\rangle \sim |\psi\rangle)$

Explaination of the bloch sphere

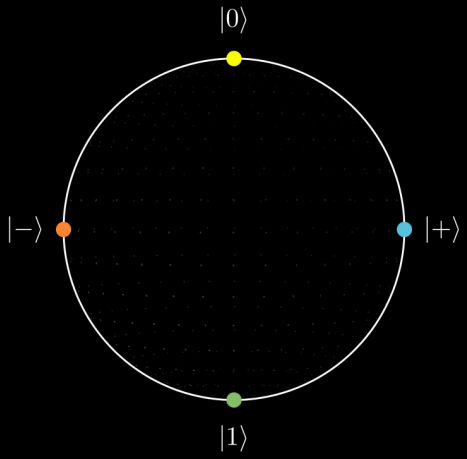


Explaination of the bloch sphere

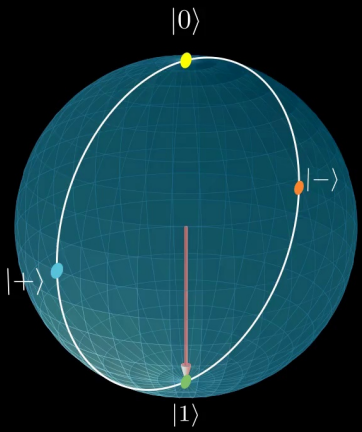


Folding the half-circle onto a full circle: $\theta_{\text{new}} = 2\,\theta_{\text{old}}$

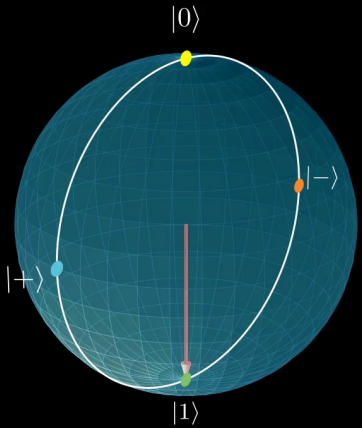
Explaination of the bloch sphere



We can similarly do this with the other dimension


$|0\rangle$
$|-\rangle$
$|+\rangle$
$|1\rangle$

Orthogonal states = antipodal points on the Bloch sphere



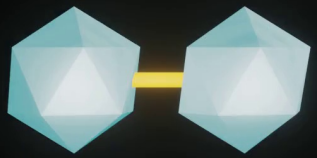
Qubits

Entanglement

$$a_0 |0\rangle + a_1 |1\rangle$$

Qubits

Entanglement



$$a_0 |0\rangle$$
$$+a_1 |1\rangle$$
$$+a_2 |2\rangle$$
$$+a_3 |3\rangle$$

Qubits

Entanglement

$$
\begin{aligned}
& a_0 \,|0\rangle \\
+ & a_1 \,|1\rangle \\
+ & a_2 \,|2\rangle \\
+ & a_3 \,|3\rangle \\
+ & a_4 \,|4\rangle \\
+ & a_5 \,|5\rangle \\
+ & a_6 \,|6\rangle \\
+ & a_7 \,|7\rangle
\end{aligned}
$$

Qubits

Entanglement

Parallelize an operation on exponentially many inputs: speedup (sometimes...)

$$
\begin{aligned}
a_0 \,|0\rangle\ |f(0)\rangle \\
+a_1 \,|1\rangle\ |f(1)\rangle \\
+a_2 \,|2\rangle\ |f(2)\rangle \\
+a_3 \,|3\rangle\ |f(3)\rangle \\
+a_4 \,|4\rangle\ |f(4)\rangle \\
+a_5 \,|5\rangle\ |f(5)\rangle \\
+a_6 \,|6\rangle\ |f(6)\rangle \\
+a_7 \,|7\rangle\ |f(7)\rangle
\end{aligned}
$$

Holevo

Holevo

NON!! (Théorème d'Holevo simplifié)

Étant donné n qubits (i.e. un état quantique de dimension 2^n), il est impossible d'extraire plus que n bits d'information.

Holevo

Mais pratique en cryptographie !

NON!! (Théorème d'Holevo simplifié)

Étant donné n qubits (i.e. un état quantique de dimension 2^n), il est impossible d'extraire plus que n bits d'information.

Holevo

Mais pratique en cryptographie !
+ il faut être malin en algorithmique !

NON!! (Théorème d'Holevo simplifié)

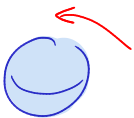
Étant donné n qubits (i.e. un état quantique de dimension 2^n), il est impossible d'extraire plus que n bits d'information.

Unitaires

Unitaires

On peut appliquer sur n'importe quel état quantique $|\psi\rangle$ n'importe quelle matrice U dite **unitaire**, i.e. telle que $U^\dagger U = I$ avec $U^\dagger$ (prononcer "dagger" la transposée conjugée). On obtient alors $U|\psi\rangle$.

Unitaires



Unitaires

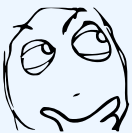
On peut appliquer sur n'importe quel état quantique $|\psi\rangle$ n'importe quelle matrice U dite **unitaire**, i.e. telle que $U^\dagger U = I$ avec $U^\dagger$ (prononcer "dagger" la transposée conjugée). On obtient alors $U|\psi\rangle$.

Unitaires

Unitaires

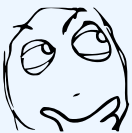
On peut appliquer sur n'importe quel état quantique $|\psi\rangle$ n'importe quelle matrice U dite **unitaire**, i.e. telle que $U^\dagger U = I$ avec $U^\dagger$ (prononcer "dagger" la transposée conjugée). On obtient alors $U|\psi\rangle$.

Comment extraire de l'information ?



Mais alors, comment **extraire** de l'information quantique pour la ramener dans le **monde classique** ?

Comment extraire de l'information ?



Mais alors, comment **extraire** de l'information quantique pour la ramener dans le **monde classique** ?

⇓

Faire des **mesures** !

Qubits

Measurement: extract information

Qubits

Measurement: extract information

Qubits

Measurement: extract information

Qubits

Measurement: extract information

1

Qubits

Measurement: extract information

1

$\Rightarrow$ not easy to exploit benefits of superposition

Qubits

Measurement: extract information

1

$\Rightarrow$ not easy to exploit benefits of superposition

Qubits

Measurement: extract information

No cloning principle

1

$\Rightarrow$ not easy to exploit benefits of superposition

Qubits

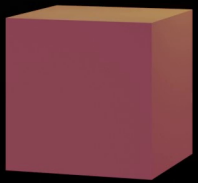
Applications

Qubits

Applications

- Shor's algorithm: factor numbers

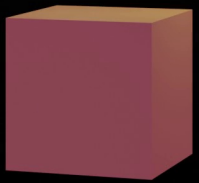
$p \times q$



Qubits

Applications

- Shor's algorithm: factor numbers



Qubits

Applications

- Shor's algorithm: factor numbers
- Grover: search efficiently an item

Qubits

Applications

- Shor's algorithm: factor numbers
- Grover: search efficiently an item

Qubits

Applications

- Shor's algorithm: factor numbers
- Grover: search efficiently an item
- ...

Impacts sur la cryptographie

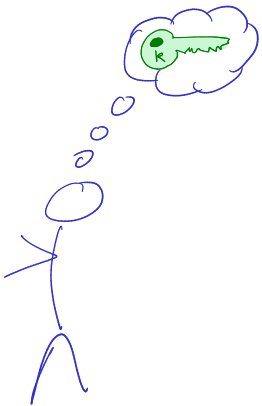
Cryptographie clé publique/privée

Chiffrement clé privée

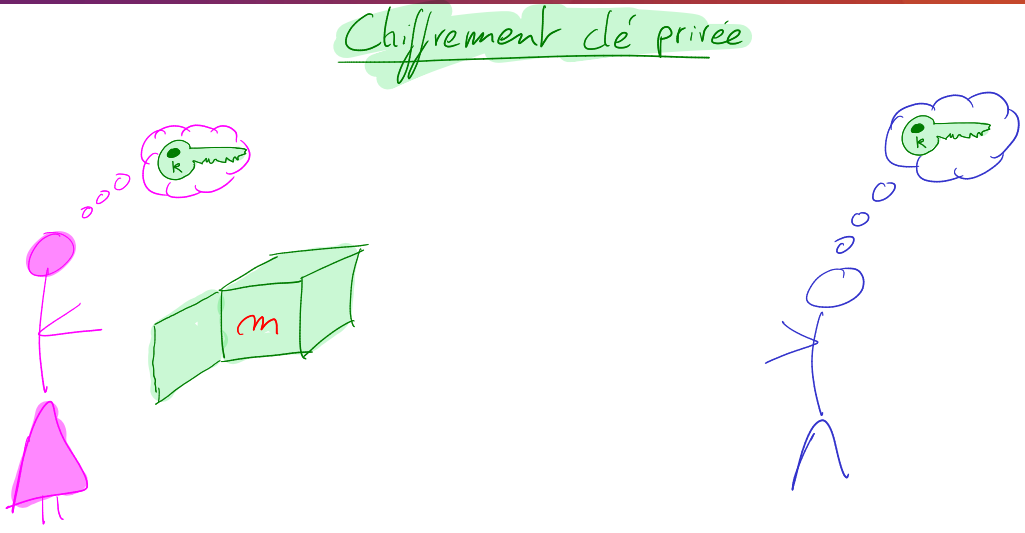
→ Penser "AES"

Cryptographie clé publique/privée

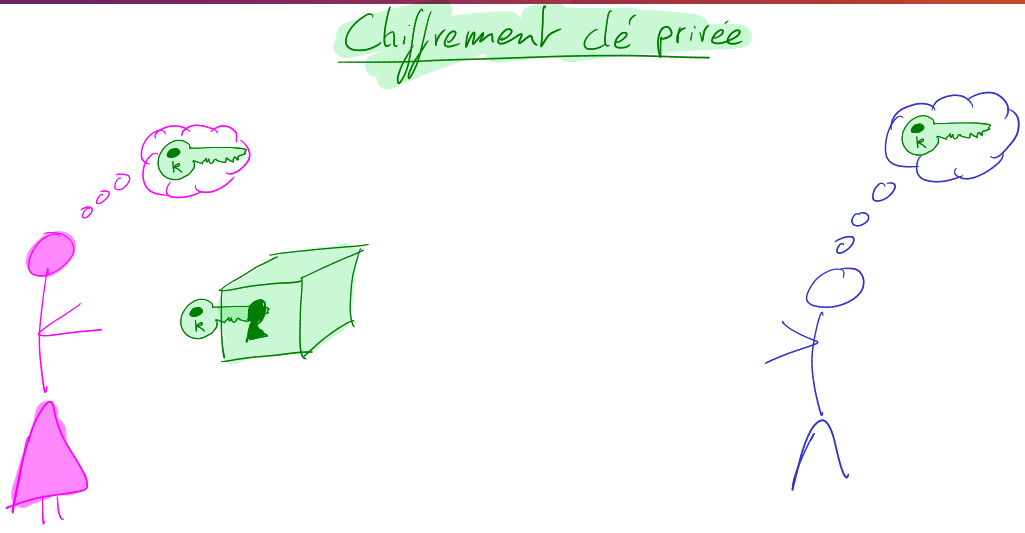
Chiffrement clé privée



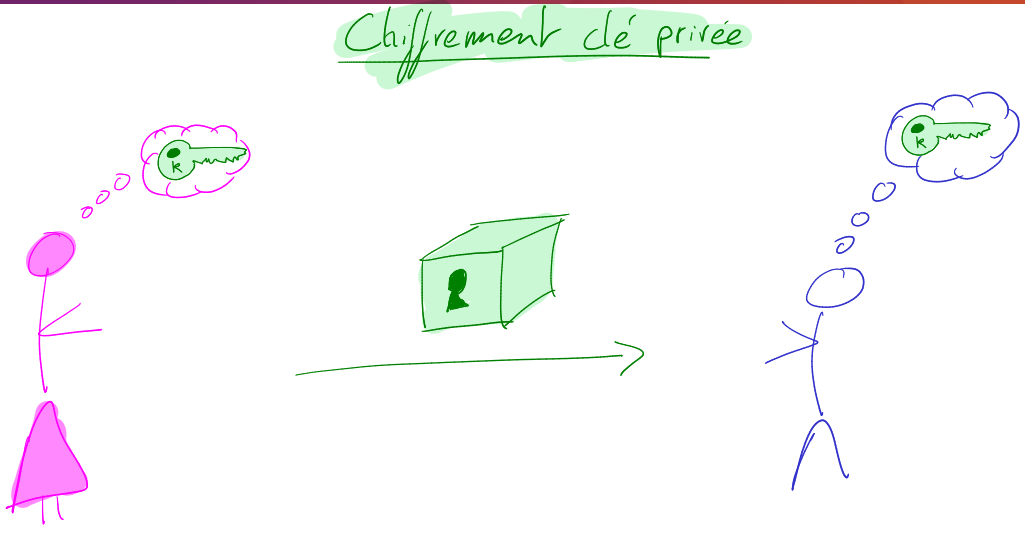
Cryptographie clé publique/privée



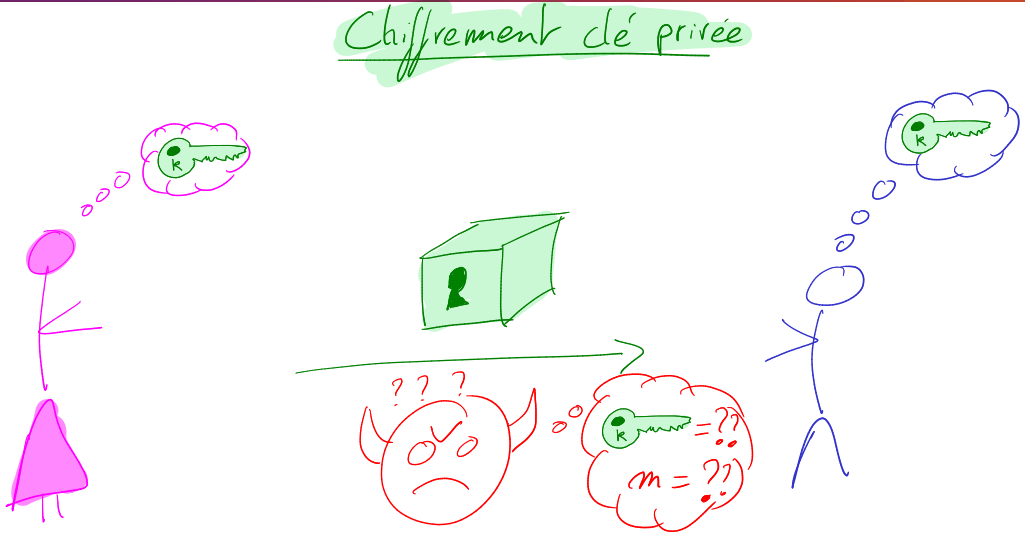
Cryptographie clé publique/privée



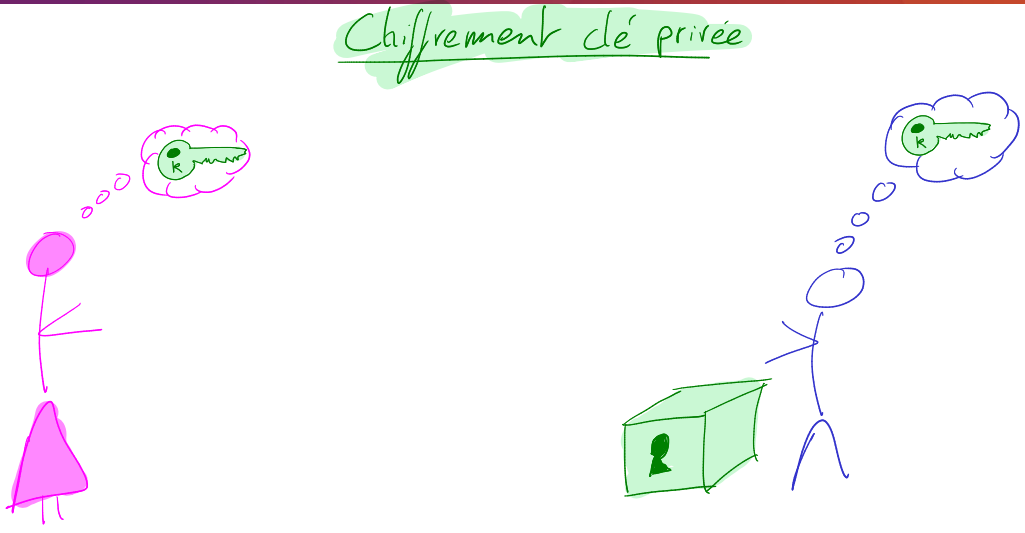
Cryptographie clé publique/privée



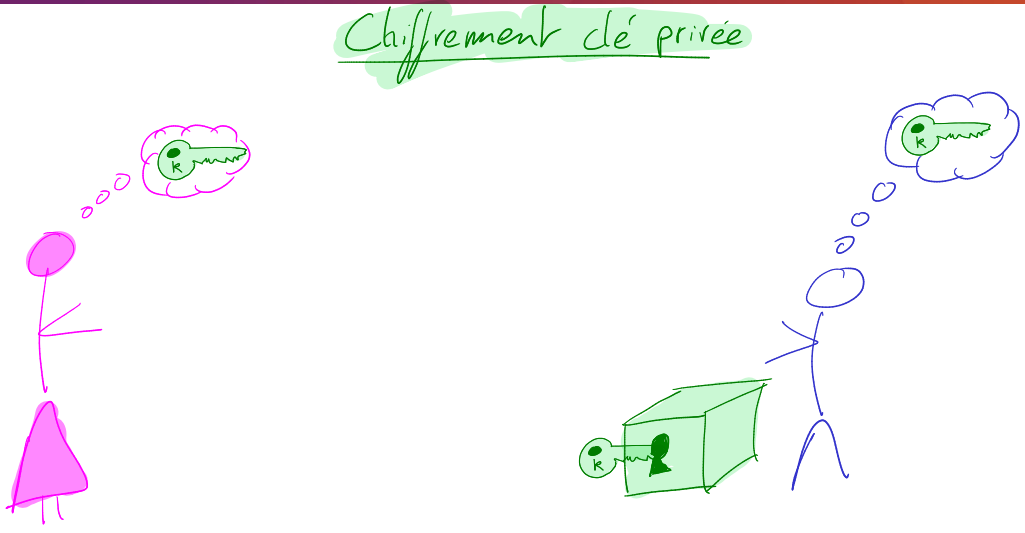
Cryptographie clé publique/privée



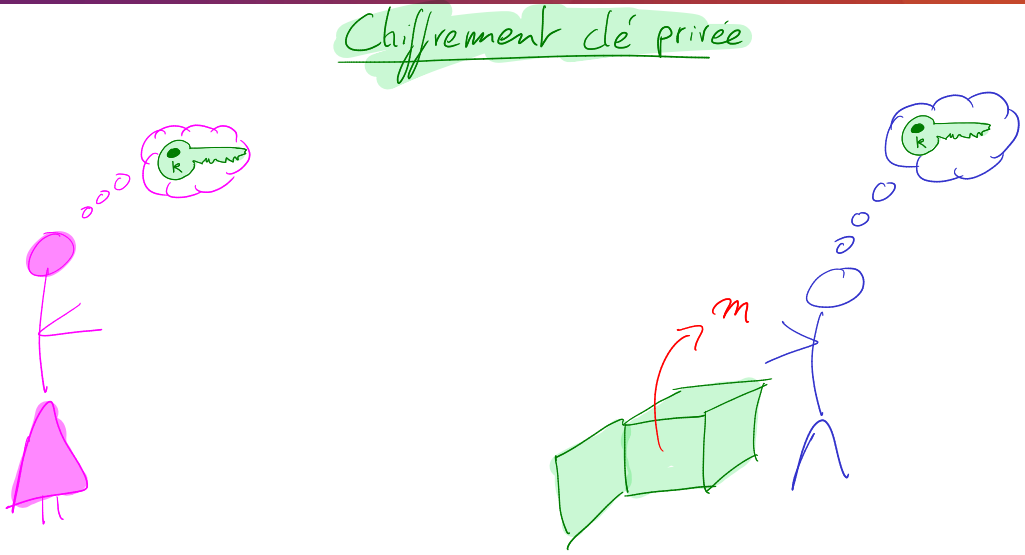
Cryptographie clé publique/privée



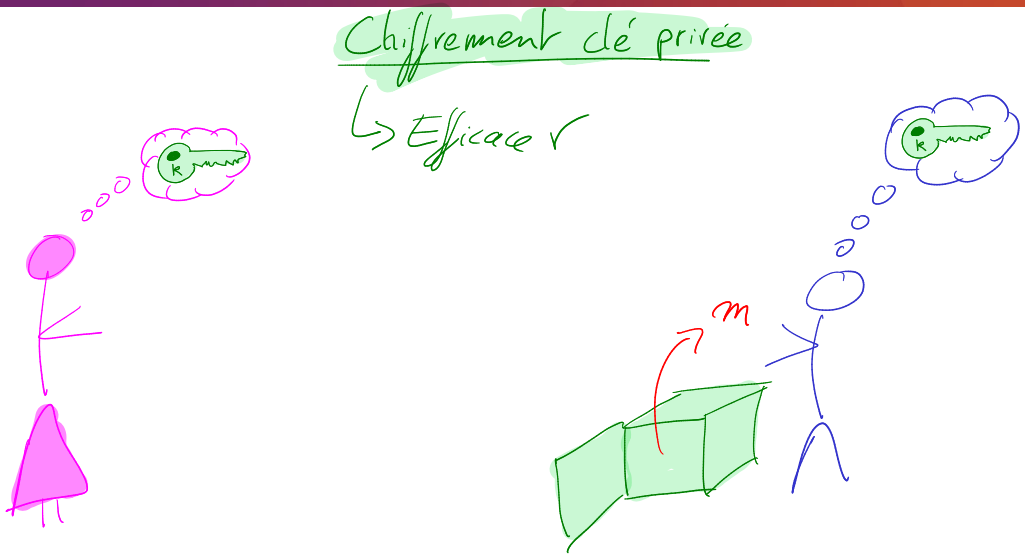
Cryptographie clé publique/privée



Cryptographie clé publique/privée



Cryptographie clé publique/privée

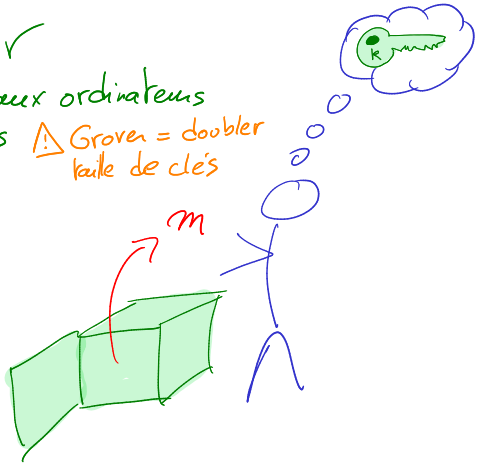


Cryptographie clé publique/privée

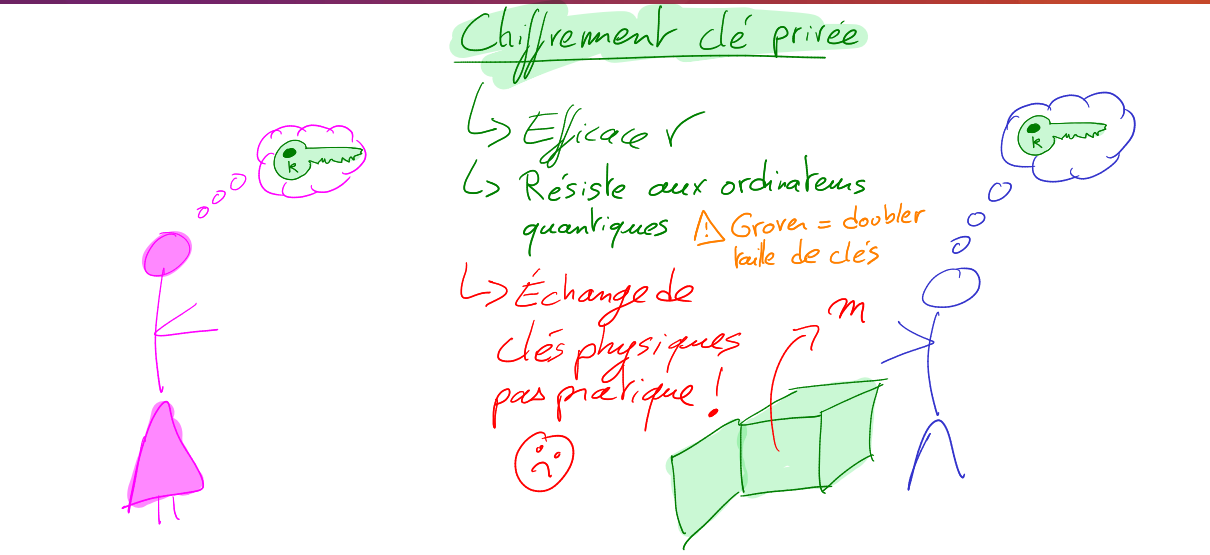
Chiffrement clé privée

↳ Efficace ✓

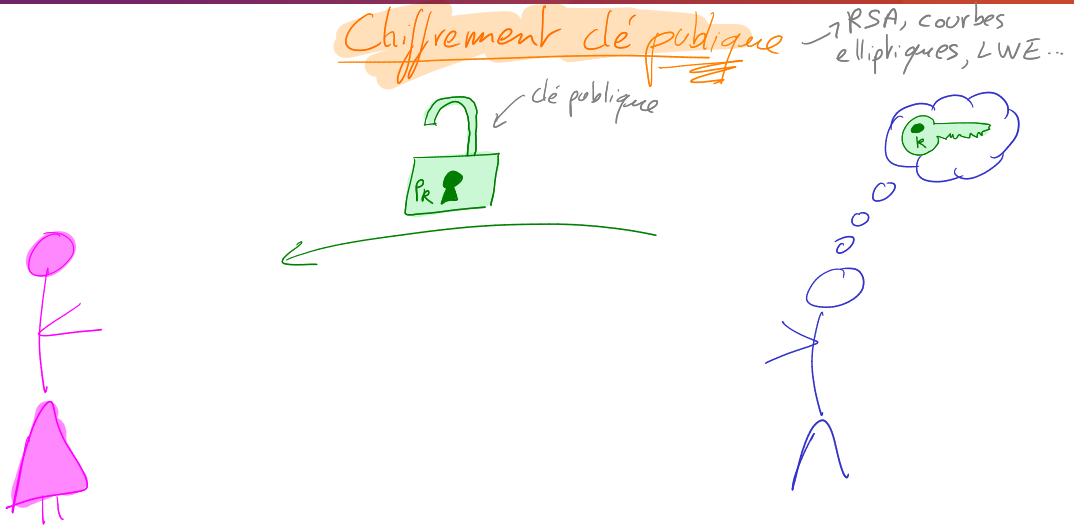
↳ Résiste aux ordinateurs quantiques ⚠ Grover = doubler taille de clés



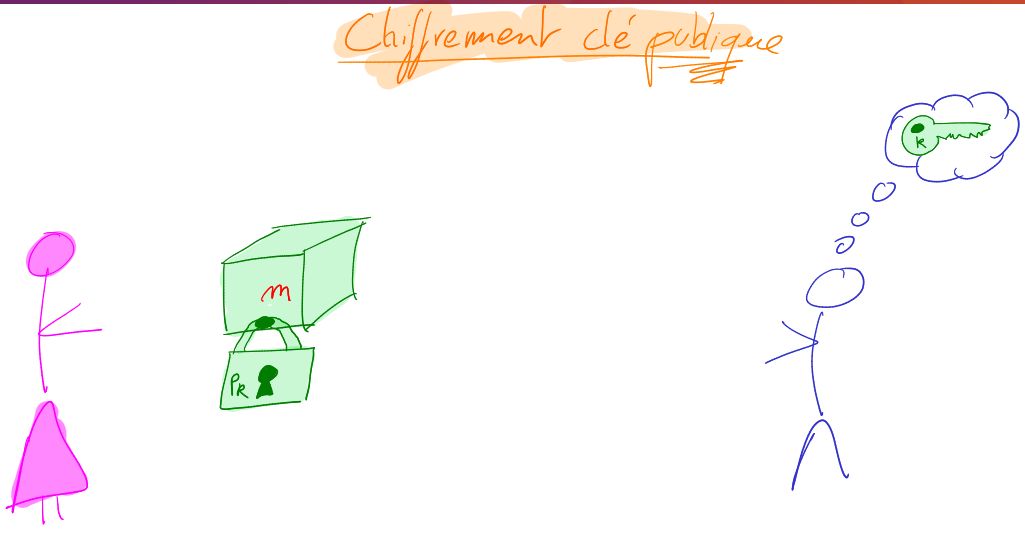
Cryptographie clé publique/privée



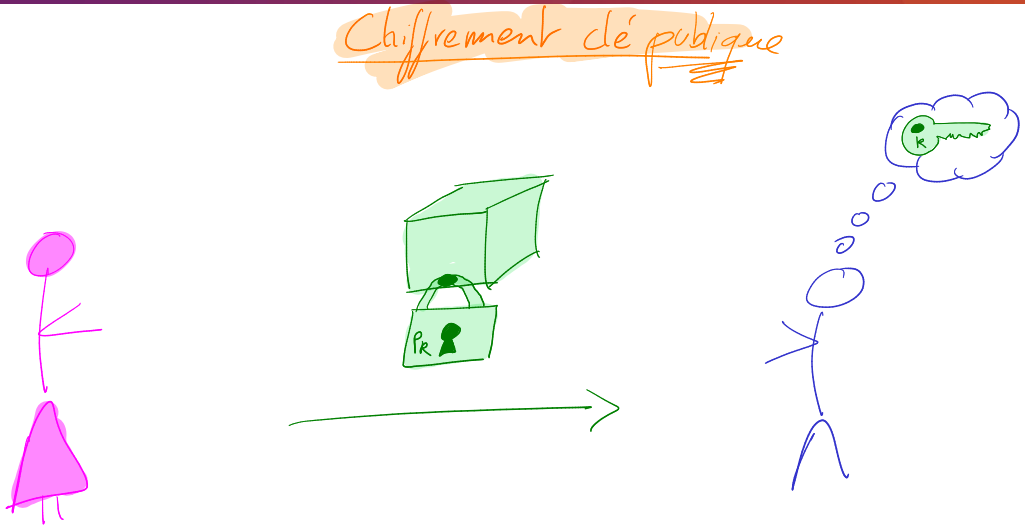
Cryptographie clé publique/privée



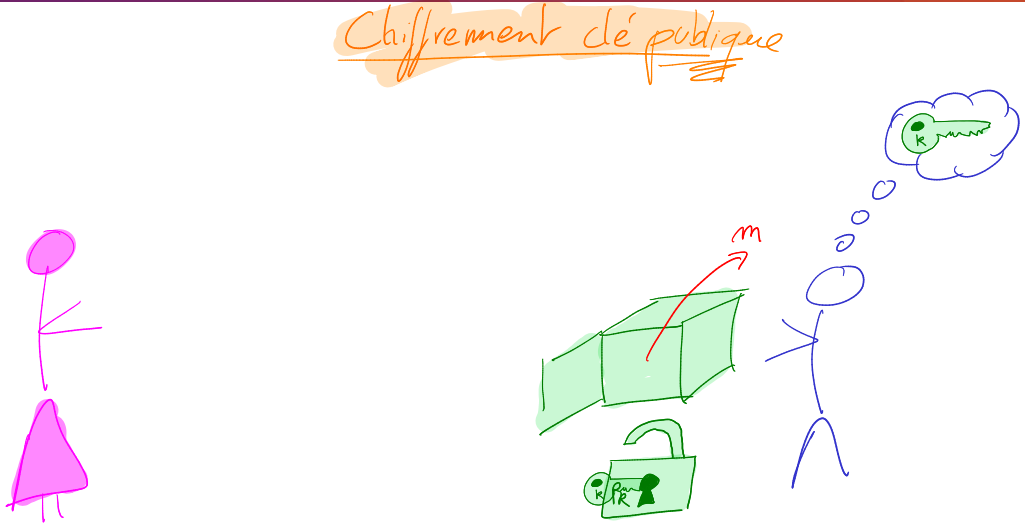
Cryptographie clé publique/privée



Cryptographie clé publique/privée



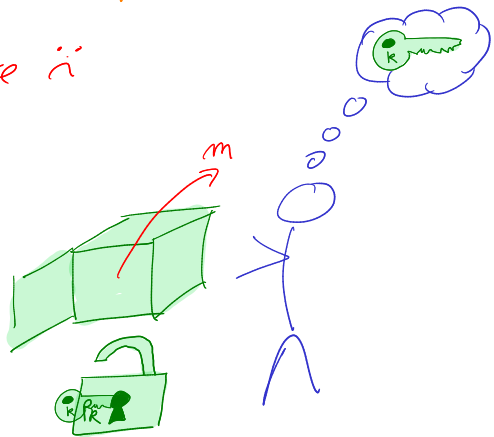
Cryptographie clé publique/privée



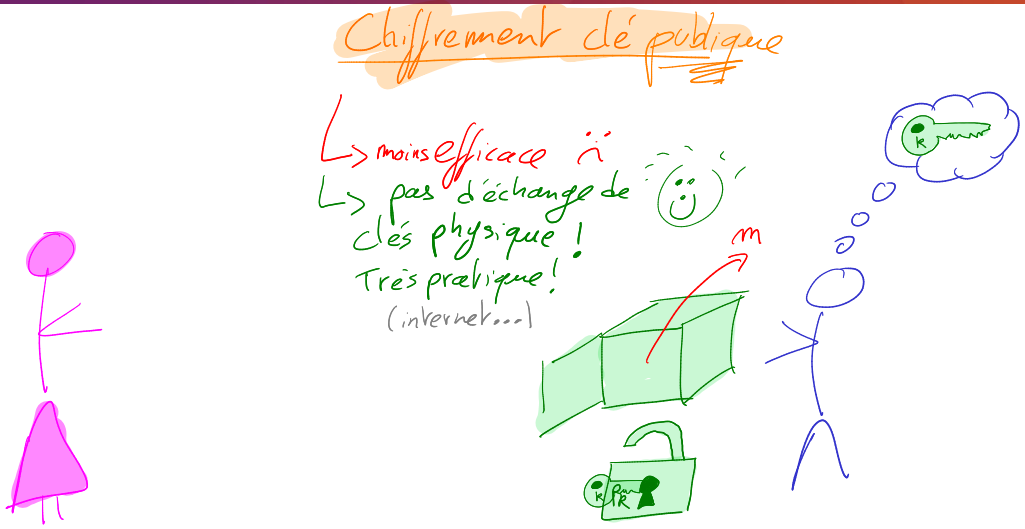
Cryptographie clé publique/privée

Chiffrement clé publique

↳ moins efficace :(



Cryptographie clé publique/privée



Cryptographie clé publique/privée

Chiffrement clé publique

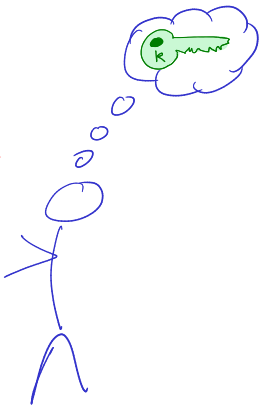
Echanger une clé (KEM) via Crypto clé publique puis utiliser chiffrement clé privée

↳ moins efficace :(

↳ pas d'échange de clés physique !

Très pratique !

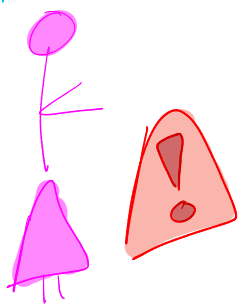
(internet...)



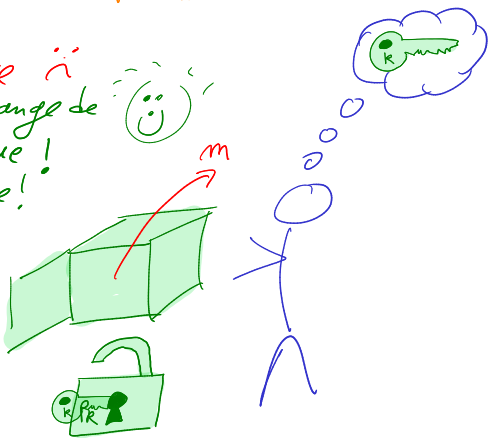
Cryptographie clé publique/privée

Chiffrement clé publique

Echanger une clé (KEM) via Crypto clé publique puis utiliser chiffrement clé privée

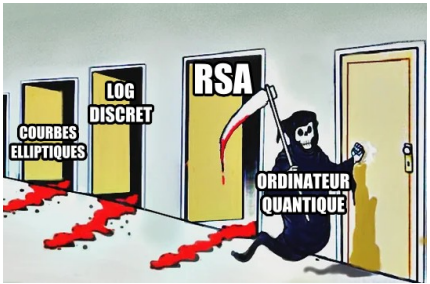


- moins efficace à
- pas d'échange de clés physique !
- Très pratique ! (internet...)
- RSA / courbes elliptiques cassées avec ordinateur quantique !!!



L'informatique quantique peut…

Détruire

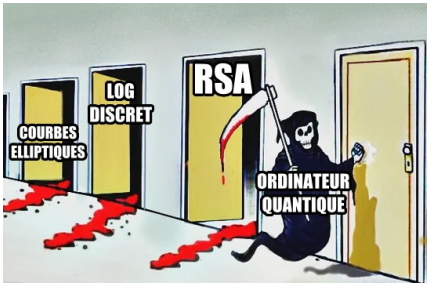


Algo de Shor = **casse toute la cryptographie** (à clé publique) utilisé aujourd'hui

Informatique quantique

L'informatique quantique peut…

Détruire



Algo de Shor = **casse toute la cryptographie** (à clé publique) utilisé aujourd'hui

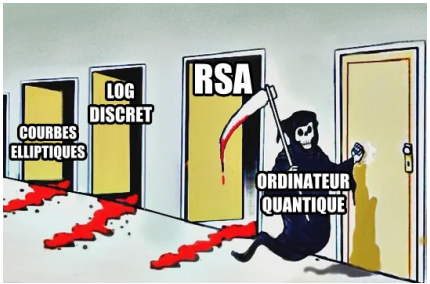
Contruire

- **Cryptographie post-quantique**
  = cryptographie classique résistant aux ordinateurs quantiques
  (réseaux euclidiens, codes, isogénies…)

Informatique quantique

L'informatique quantique peut…

Détruire



Algo de Shor = **casse toute la cryptographie** (à clé publique) utilisé aujourd'hui

Contruire

- **Cryptographie post-quantique**
  = cryptographie classique résistant aux ordinateurs quantiques
  (réseaux euclidiens, codes, isogénies…)
- **Cryptographie quantique**
  = entre ordinateur quantiques, sécurisé "à tout jamais"
  (distribution quantique de clé QKD…)

Ordinateur quantique : la quête du Graal

Ordinateur quantique : acteurs et financements

Le Plan Quantique, ambitieux et attendu

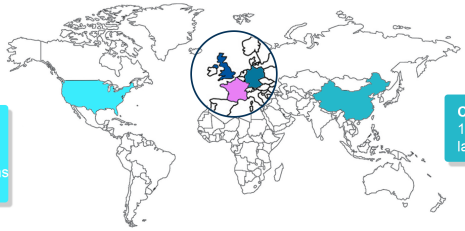
Quelques investissements gouvernementaux dans les technologies quantiques autour du globe.

UE : Flagship Quantique
1 Md€ sur 10 ans
lancé en 2018

Royaume-Uni
1 Md£ sur 10 ans
lancé en 2014

France : Plan Quantique
1,8 Md€ sur 5 ans
lancé en 2021

Allemagne
650 M€ sur 5 ans
lancé en 2018
+ 2 Md€ en 2020



Etats-Unis
1,3 Md$ sur 5 ans
lancé en 2018
+ 800 M$ sur 2 ans
en mars 2020

Chine
10 Md€
lancé en 2015

© CNRS - Source : sites gouvernementaux, rapport Forteza et Olivier Ezratty

QUANTINUUM

Microsoft

quobly

IBM

Google

XANADU

PsiQuantum

rigetti

QUANDELA

ALICE & BOB

VeriQloud

PASQAL

Ordinateur quantique : acteurs et financements

Emmanuel Macron annonce 1,55 milliard d'euros de plus pour la filière quantique et les semi-conducteurs

Ces annonces s'ajoutent au plan Quantique de 1,8 milliard d'euros sur la période 2021-2025, complété en 2024 par 500 millions d'euros via un programme pour accompagner en commande publique le secteur de la défense.

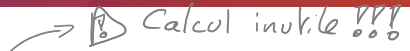
Le Monde avec AFP
Publié le 22 mai 2026 à 11h11, modifié le 22 mai 2026 à 13h23 · Lecture 3 min.

Le président de la République, Emmanuel Macron, à l'Elysée, à Paris, le jeudi 21 mai 2026. THIBAULT CAMUS/AP

Ordinateur quantique : la quête du Graal

2019 : Google affirme avoir atteint la **« suprématie quantique »** (53 qubits)

Ordinateur quantique : la quête du Graal



2019 : Google affirme avoir atteint la **« suprématie quantique »** (53 qubits)

Ordinateur quantique : la quête du Graal

2019 : Google affirme avoir atteint la **« suprématie quantique »** (53 qubits)

$\Rightarrow$ **Contestation par IBM !**

Ordinateur quantique : la quête du Graal

2019 : Google affirme avoir atteint la **« suprématie quantique »** (53 qubits)

⇒ **Contestation par IBM !**

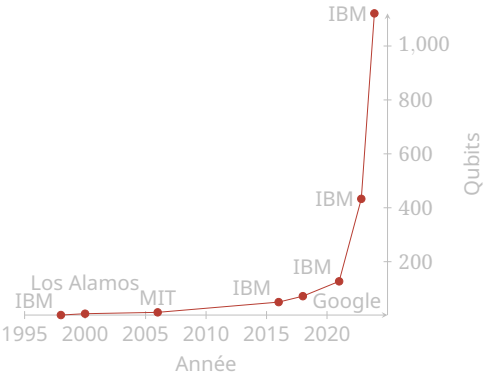
Comment vérifier que le calcul n'est pas accessible à des ordinateurs classiques ?

(sujet de recherche actif)

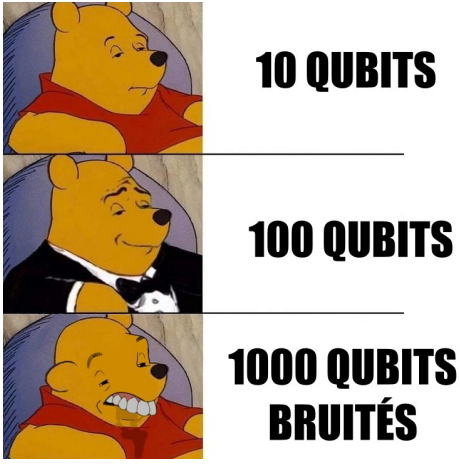
Ordinateur quantique : la quête du Graal

2019 : Google affirme avoir atteint la **« suprématie quantique »** (53 qubits)

⇒ **Contestation par IBM !**

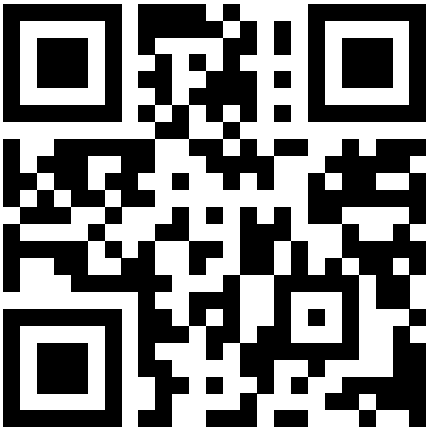


Ordinateur quantique : le problème du bruit



Problème :
Très sensible au bruit !!!

Ordinateur quantique : le problème du bruit



Problème :
Très sensible au bruit !!!

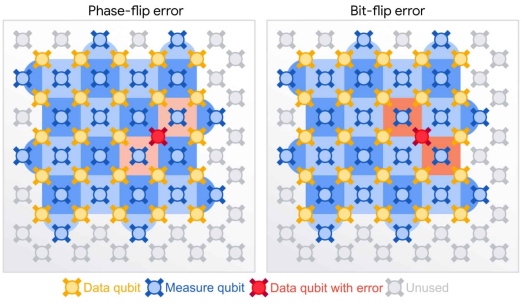
⇒ **Solution** :
Correction d'erreurs (ECC)

Ordinateur quantique : le problème du bruit

Problème :
Très sensible au bruit !!!

⇒ **Solution** :
Correction d'erreurs (ECC)

Ordinateur quantique : le problème du bruit

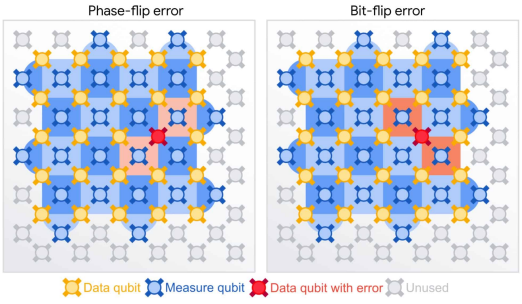


Problème :
Très sensible au bruit !!!

⇒ **Solution** :
Correction d'erreurs (ECC)

Attention : pas facile !
(ECC = + de portes = + de bruit)

Ordinateur quantique : le problème du bruit



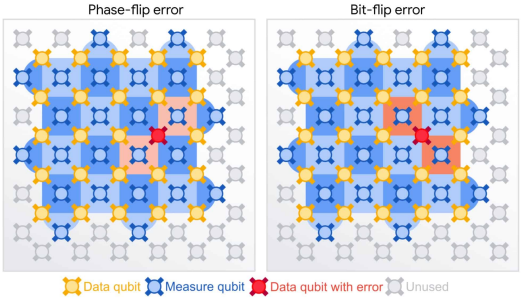
Problème :
Très sensible au bruit !!!

⇒ **Solution** :
Correction d'erreurs (ECC)

Attention : pas facile !
(ECC = + de portes = + de bruit)

⇒ **Threshold** theorem

Ordinateur quantique : le problème du bruit



Problème :
Très sensible au bruit !!!

⇒ **Solution** :
Correction d'erreurs (ECC)

Attention : pas facile !
(ECC = + de portes = + de bruit)

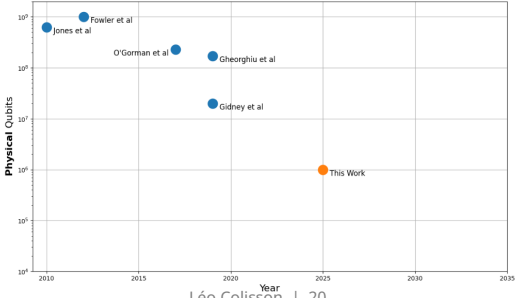
⇒ **Threshold** theorem

En pratique
2024 : Quantinuum/Microsoft
= qubits logiques > physiques
juin 2025 : démonstration par

Améliorations matérielles & logicielles

Récentes améliorations importantes dans l'efficacité de Shor :

- Shor (1994) $\approx \tilde{O}(\log^3 N)$
- Regev (2024) $\approx \tilde{O}(\log^{3/2} N)$ quantum gates + polynomial classical post-processing
- Gidney (2024) *How to factor 2048 bit RSA integers with less than a million noisy qubits* Assumptions: "a square grid of qubits with nearest neighbor connections, a uniform gate error rate of 0.1%, a surface code cycle time of 1 microsecond, and a control system reaction time of 10 microseconds."



Ordinateur quantique : pourquoi s'inquiéter maintenant ?

? S'il n'existe pas encore d'ordinateur quantique,
pourquoi s'inquiéter maintenant?

Ordinateur quantique : pourquoi s'inquiéter maintenant ?

?

S'il n'existe pas encore d'ordinateur quantique,
pourquoi s'inquiéter maintenant?

"Récolter maintenant, déchiffrer plus tard" !!

Ordinateur quantique : pourquoi s'inquiéter maintenant ?

Motivations

On ne peut donc **pas attendre**…

Problème : RSA/ECDSA/… bien plus étudiés que la cryptographie post-quantique ! (E.g. SIKE cassé !)

Motivations

On ne peut donc **pas attendre**…

Problème : RSA/ECDSA/… bien plus étudiés que la cryptographie post-quantique ! (E.g. SIKE cassé !)

- Création d'une **compétition internationale** NIST
  (Objectif : trouver les meilleurs chiffrements/signatures = efficaces & sécurisés)

Motivations

On ne peut donc **pas attendre**…

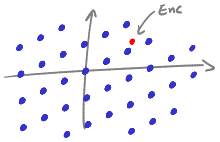
Problème : RSA/ECDSA/… bien plus étudiés que la cryptographie post-quantique ! (E.g. SIKE cassé !)

- Création d'une **compétition internationale** NIST (Objectif : trouver les meilleurs chiffrements/signatures = efficaces & sécurisés)
- Pour l'instant, **combiner** RSA/… & post-quantique?

Cryptographie post-quantique

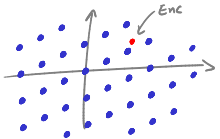
Famous post-quantum candidates

1. Lattice-based Crypto

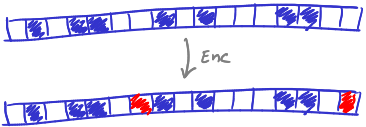


Famous post-quantum candidates

1 Lattice-based Crypto

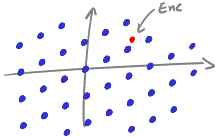


2 Code-based Crypto

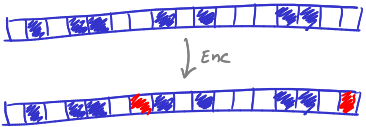


Famous post-quantum candidates

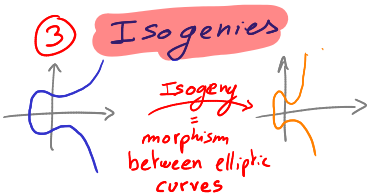
1 Lattice-based Crypto



2 Code-based Crypto

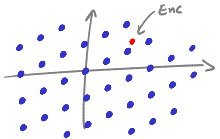


3 Isogenies

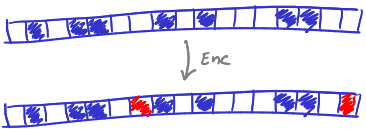


Famous post-quantum candidates

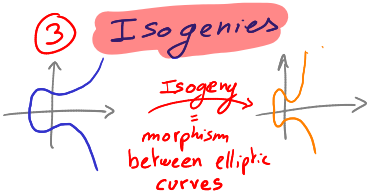
1 Lattice-based Crypto



2 Code-based Crypto



3 Isogenies

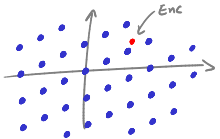


4 Multivariate Crypto

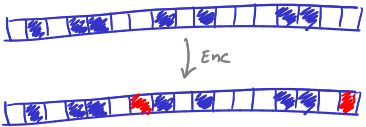
$$P_k := \begin{cases} \bullet\ 1 + x_1 + 2x_0x_3 \\ \bullet\ 4 + x_4 + 3x_1^2x_8 + x_9 \\ \bullet\ x_6 + x_2^3x_5 + x_7x_5 \end{cases} \xrightarrow{\text{Enc}} P_k(m)$$

Famous post-quantum candidates

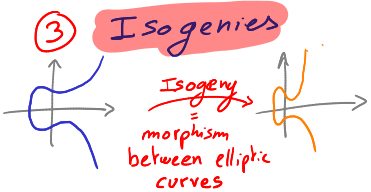
1. Lattice-based Crypto



2. Code-based Crypto



3. Isogenies



4. Multivariate Crypto

$$P_k := \begin{cases} \cdot\ 1 + x_1 + 2x_0x_3 \\ \cdot\ 4 + x_4 + 3x_1^2x_8 + x_9 \\ \cdot\ x_6 + x_2^3x_5 + x_7x_5 \end{cases} \xrightarrow{\text{Enc}} P_k(m)$$

5. + Symmetric crypto (incl. signatures)

Famous post-quantum candidates

1 Lattice-based Crypto

- ✓ studied extensively
- ✓ efficient
- ✓ simple
- ✓ versatile (FHE ...)
- ✓ hard also on average !

2 Code-based Crypto

- ✓ simple
- ✗ no worst case → average case reduction
- ✗ FHE impossible

3 Isogenies

- ✗ SIDH broken => lost confidence
- ✗ complicated

4 Multivariate Crypto

- ✗ many candidates were broken => lost confidence

5 + Symmetric crypto (incl. signatures)

Famous post-quantum candidates

1 Lattice-based Crypto

- ✓ studied extensively
- ✓ efficient
- ✓ simple
- ✓ versatile (FHE ...)
- ✓ hard also on average !

2 Code-based Crypto

- ✓ simple
- ✗ no worst case → average case reduction
- ✗ FHE impossible

3 Isogenies

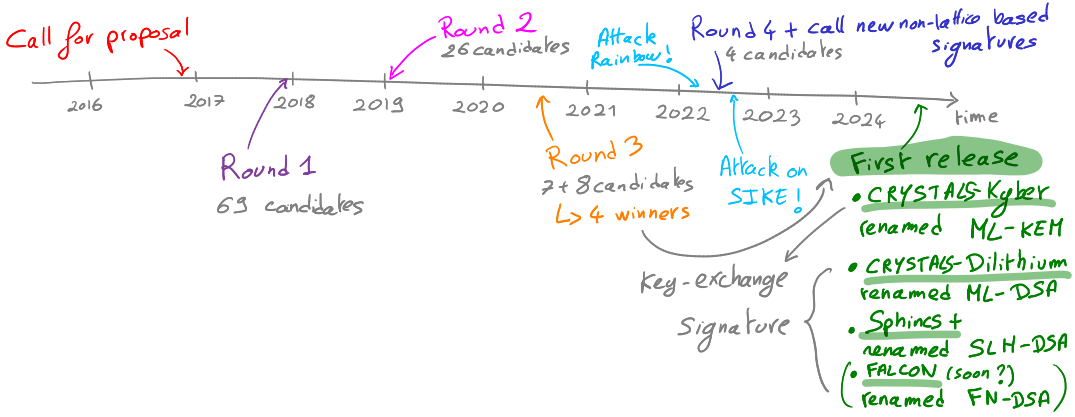
- ✗ SIDH broken => lost confidence
- ✗ complicated

4 Multivariate Crypto

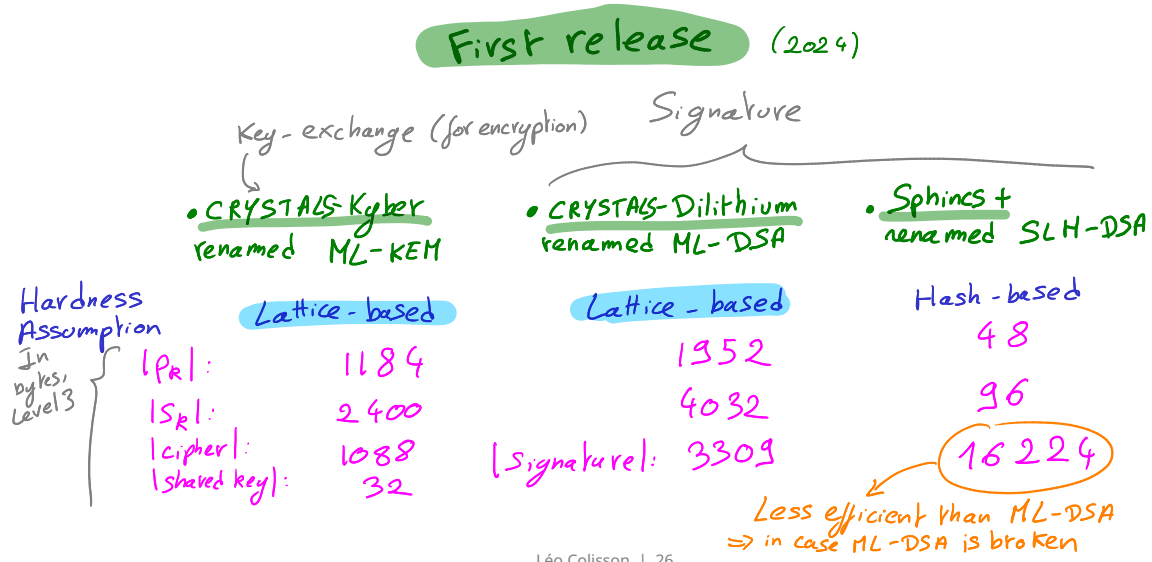
- ✗ many candidates were broken => lost confidence

5 + Symmetric crypto (incl. signatures)

NIST : compétition post-quantique internationale



NIST : compétition post-quantique internationale



NIST : compétition post-quantique internationale

First release (2024)

Key-exchange (for encryption)

- CRYSTALS-Kyber
  renamed ML-KEM

Compare with ECDH with Curve 25519
(Not post-quantum !)

Hardness Assumption	Lattice-based ✓	Elliptic-curves ✗
In bytes, Level 3		
$\lvert pk \rvert$:	1184 ✗	32 ✓
$\lvert sk \rvert$:	2400 ✗	32 ✓
$\lvert$cipher$\rvert$:	1088 ✗	64 (2x32) ✓
$\lvert$shared key$\rvert$:	32 ✗	32 ✓

NIST : compétition post-quantique internationale

First release (2024)

Key-exchange (for encryption)

- CRYSTALS-Kyber
  renamed ML-KEM

Compare with ECDH with Curve 25519
(Not post-quantum !)

Hardness Assumption: Lattice-based ✓ | Elliptic-curves ✗

In bytes, Level 3

$\lvert pk \rvert$:	1184 ✗	32 ✓
$\lvert sk \rvert$:	2400 ✗	32 ✓
$\lvert cipher \rvert$:	1088 ✗	64 (2×32) ✓
$\lvert shared\ key \rvert$:	32 ✗	32 ✓

Post-quantum is less efficient (but hopefully more secure)

NIST : compétition post-quantique internationale

Est-ce grave si les systèmes post-quantiques sont moins efficaces ?

?

NIST : compétition post-quantique internationale

?

Est-ce grave si les systèmes post-quantiques sont moins efficaces ?

⇒ Souvent, pas vraiment car en pratique **chiffrement hybride**
(crypto clé publique seulement pour échanger la clé, puis crypto clé privée car + efficace)

NIST : déploiement

Migration vers le post-quantique : recommandations **officielles**

- USA : 16 janvier 2025 : décret 14144 de Joe Biden = transition avant 2030
- Commission Européenne/NIS :
  “All Member States should start transitioning to post-quantum cryptography by the end of 2026. At the same time, the protection of critical infrastructures should be transitioned to PQC **as soon as possible**, no later than **by the end of 2030**.”
  `https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography`

Le déploiement, c’est **maintenant** !

NIST : déploiement

- **Timing** : « *L'ANSSI conseille aux organisations publiques et privées de démarrer **dès à présent** un premier travail d'inventaire […] L'ANSSI indique qu'il ne sera pas raisonnable d'acheter des produits qui n'intègrent pas de la PQC après 2030. Par ailleurs, l'ANSSI vise la mise en place **d'obligations PQC** pour l'entrée en qualification de produits à partir de **2027**.* »
- **Crypto-agilité** : « *L'ANSSI recommande très fortement que les produits soient capables de **changer de jeux de paramètres** pour les algorithmes de cryptographie post-quantique standardisés par le NIST.* »
- **Hybridation** : « *L'ANSSI insiste fortement sur le **caractère essentiel de l'hybridation** des algorithmes de cryptographie post-quantique partout où ils sont déployés.* »

Sources et pointeur pour avoir plus de recommandations :

`https://cyber.gouv.fr/enjeux-technologiques/cryptographie-post-quantique/faq-pqc/`

NIST : déploiement en pratique ?

NIST : FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA)
(`https://csrc.nist.gov/pubs/fips/203/final`)

TLS : Brouillon X25519MLKEM768 (hybride X25519 + MLKEM) et 2 autres modèles plus fort, mais déjà largement déployé (Firefox, Chrome, OpenSSL (3.5), Amazon…)

Cloudflare : mesure sur son réseau **50% du trafic humain post-quantique**. **Les clients sont prêts !**

OpenSSH : par défaut depuis OpenSSH 10.0 (Avril 2025), via mlkem768x25519-sha256, (pour chiffrement seulement, signature moins pressante)

NIST : déploiement en pratique ?

Essai pratique via `ssh -v ...` :

```
debug1: kex: algorithm: mlkem768x25519-sha256
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
```

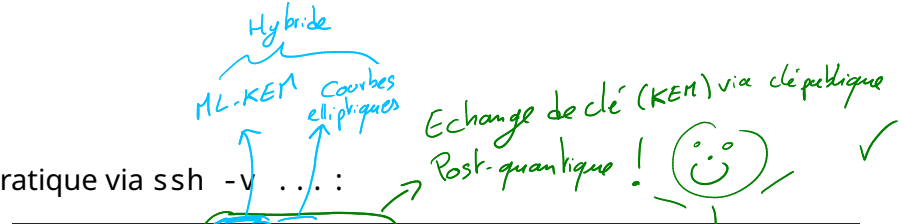
NIST : déploiement en pratique ?

Essai pratique via `ssh -v ...` :


```
debug1: kex: algorithm: mlkem768x25519-sha256
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
```

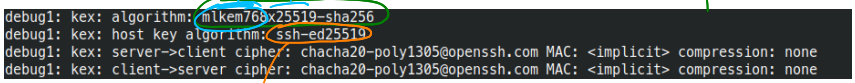
NIST : déploiement en pratique ?

Essai pratique via `ssh -v ...` :



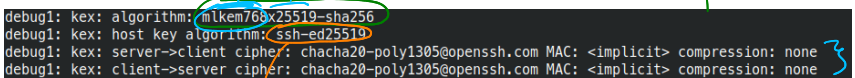
NIST : déploiement en pratique ?

Essai pratique via `ssh -v ...` :



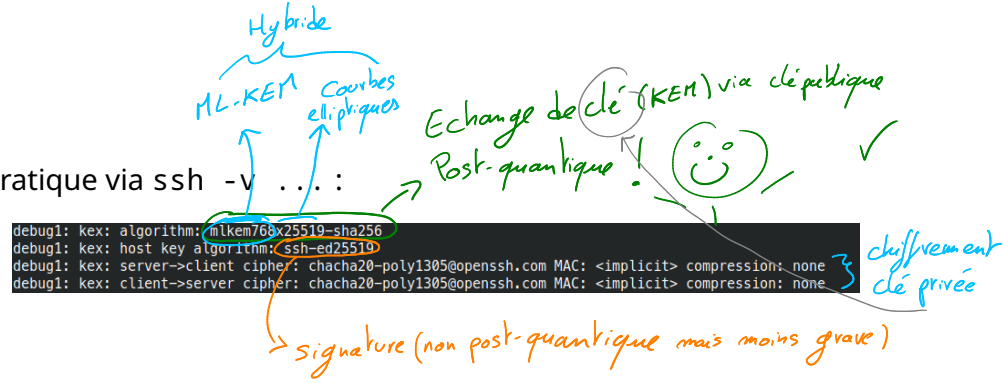
NIST : déploiement en pratique ?

Essai pratique via `ssh -v ...` :



NIST : déploiement en pratique ?

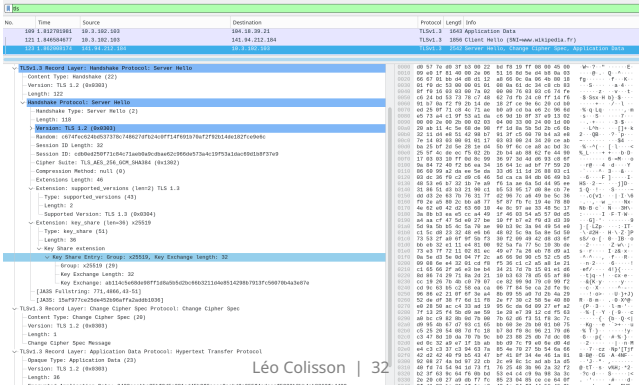
Essai pratique via `ssh -v ...` :



NIST : déploiement en prance ?

Quelques essais sur navigateur (Firefox et Chrome) via wireshark :

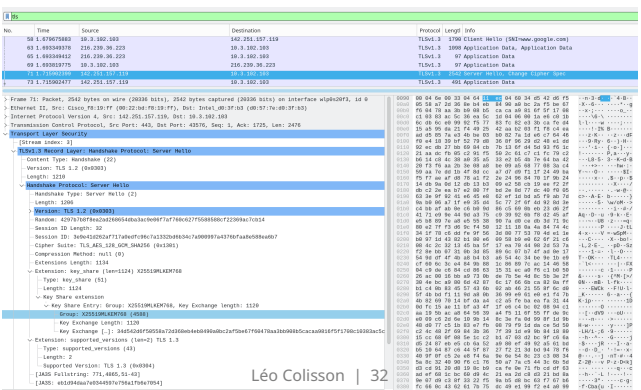
- `wikipedia.fr` ne supporte pas X25519MLKEM768 ✘



NIST : déploiement en pratique ?

Quelques essais sur navigateur (Firefox et Chrome) via wireshark :

- `wikipedia.fr` ne supporte pas X25519MLKEM768 ✘
- `google.com` et `cloudflare.com` utilisent X25519MLKEM768… et également `fr.wikipedia.org` et mon instance nextcloud privée ! ✓



NIST : déploiement des signatures

Signatures (ML-DSA/SLH-DSA)
= **beaucoup moins bien supportées dans TLS** que chiffrement
+ **sans implémentation existante** !

(moins pressant: pas sensible au “récolter maintenant, déchiffrer plus tard”)…

Mais il faudra y passer un jour !

- `https://datatracker.ietf.org/doc/draft-ietf-tls-mldsa/`
- `https://datatracker.ietf.org/doc/draft-reddy-tls-composite-mldsa/` (version hybride)
- `https://datatracker.ietf.org/doc/draft-reddy-tls-slhdsa/`

À vous de jouer !

Quand mon patron me demande
si notre infra est post-quantique

Cryptographie quantique

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Objectifs : cryptographie impossible classiquement

- Sécurité **inconditionnelle**/everlasting security
  (adversaire non borné calculatoirement/après le protocole)

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Objectifs : cryptographie impossible classiquement

- Sécurité **inconditionnelle**/everlasting security
  (adversaire non borné calculatoirement/après le protocole)
- Utiliser des **hypothèses de sécurité moins fortes**
  (MiniQCrypt, fonctions de hachage, Pseudo-Random States…)

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Objectifs : cryptographie impossible classiquement

- Sécurité **inconditionnelle**/everlasting security
  (adversaire non borné calculatoirement/après le protocole)
- Utiliser des **hypothèses de sécurité moins fortes**
  (MiniQCrypt, fonctions de hachage, Pseudo-Random States…)
- **Primitives impossibles** classiquement
  (vérification de position, monnaie quantique unclonable…)

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Objectifs : cryptographie impossible classiquement

- Sécurité **inconditionnelle**/everlasting security
  (adversaire non borné calculatoirement/après le protocole)
- Utiliser des **hypothèses de sécurité moins fortes**
  (MiniQCrypt, fonctions de hachage, Pseudo-Random States…)
- **Primitives impossibles** classiquement
  (vérification de position, monnaie quantique unclonable…)
- **Certifier le caractère quantique** d'un ordinateur

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Objectifs : cryptographie impossible classiquement

- Sécurité **inconditionnelle**/everlasting security
  (adversaire non borné calculatoirement/après le protocole)
- Utiliser des **hypothèses de sécurité moins fortes**
  (MiniQCrypt, fonctions de hachage, Pseudo-Random States…)
- **Primitives impossibles** classiquement
  (vérification de position, monnaie quantique unclonable…)
- **Certifier le caractère quantique** d'un ordinateur
- Équivalents quantiques de protocoles classiques
  (**calcul délégué** sécurisé/multipartite, vérification, …)

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Objectifs : cryptographie impossible classiquement

- Sécurité **inconditionnelle**/everlasting security
  (adversaire non borné calculatoirement/après le protocole)
- Utiliser des **hypothèses de sécurité moins fortes**
  (MiniQCrypt, fonctions de hachage, Pseudo-Random States…)
- **Primitives impossibles** classiquement
  (vérification de position, monnaie quantique unclonable…)
- **Certifier le caractère quantique** d'un ordinateur
- Équivalents quantiques de protocoles classiques
  (**calcul délégué** sécurisé/multipartite, vérification, …)
- **Preuves** de sécurité contre adversaires quantiques

Cryptographie quantique

Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Objectifs : cryptographie impossible classiquement

- Sécurité **inconditionnelle**/everlasting security
  (adversaire non borné calculatoirement/après le protocole)
- Utiliser des **hypothèses de sécurité moins fortes**
  (MiniQCrypt, fonctions de hachage, Pseudo-Random States…)
- **Primitives impossibles** classiquement
  (vérification de position, monnaie quantique unclonable…)
- **Certifier le caractère quantique** d'un ordinateur
- Équivalents quantiques de protocoles classiques
  (**calcul délégué** sécurisé/multipartite, vérification, …)
- **Preuves** de sécurité contre adversaires quantiques
- …

Cryptographie quantique

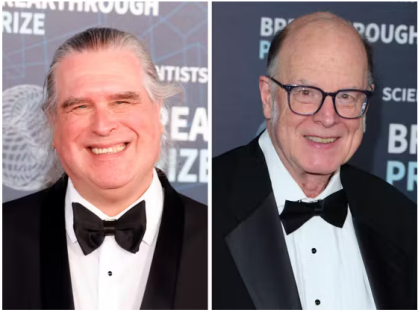
Cryptographie quantique = crypto basée sur les **lois de la physique**
(e.g. théorème non clonage)

Objectifs : cryptographie impossible classiquement

Notre focus

- Sécurité **inconditionnelle**/everlasting security
  (adversaire non borné calculatoirement/après le protocole)
- Utiliser des **hypothèses de sécurité moins fortes**
  (MiniQCrypt, fonctions de hachage, Pseudo-Random States…)
- **Primitives impossibles** classiquement
  (vérification de position, monnaie quantique unclonable…)
- **Certifier le caractère quantique** d'un ordinateur
- Équivalents quantiques de protocoles classiques
  (**calcul délégué** sécurisé/multipartite, vérification, …)
- **Preuves** de sécurité contre adversaires quantiques
- …

Exemple d’application : distribution quantique de clés (QKD)



A gauche, Gilles Brassard ; à droite, Charles H. Bennett, tous les deux à Los Angeles, le 15 avril 2023. TAYLOR HILL VIA GETTY IMAGES/JUAN PABLO RICO/AFP

Exemple d'application : distribution quantique de clés (QKD)

A gauche, Gilles Brassard ; à droite, Charles H. Bennett, tous les deux à Los Angeles, le 15 avril 2023. TAYLOR HILL VIA GETTY IMAGES/JUAN PABLO RICO/AFP

Prix Turing (2026)

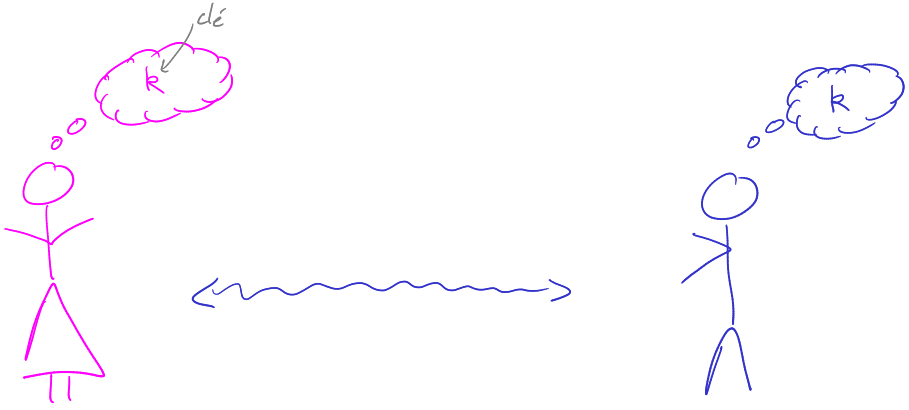
Exemple d'application : distribution quantique de clés (QKD)

BB84 année

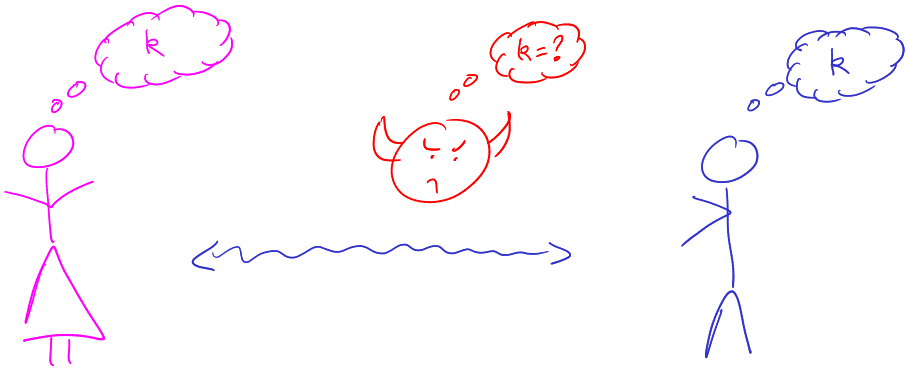
A gauche, Gilles Brassard ; à droite, Charles H. Bennett, tous les deux à Los Angeles, le 15 avril 2023. TAYLOR HILL VIA GETTY IMAGES/JUAN PABLO RICO/AFP

Prix Turing (2026)

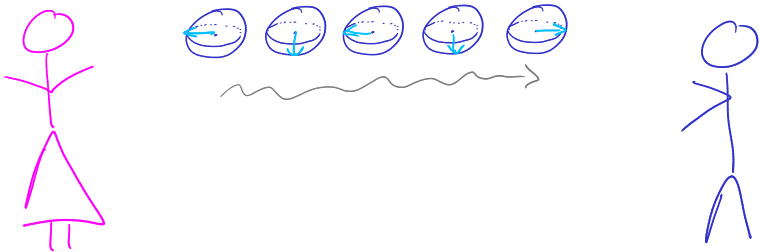
Exemple d'application : distribution quantique de clés (QKD)



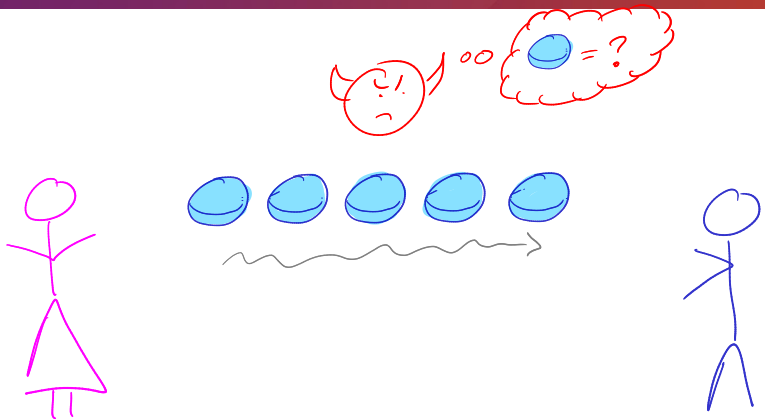
Exemple d'application : distribution quantique de clés (QKD)



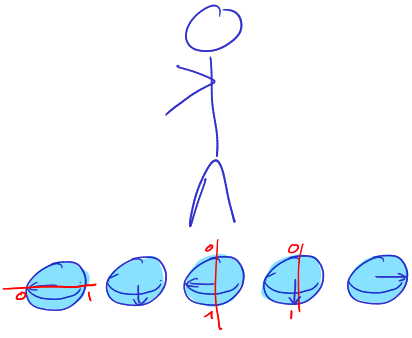
Exemple d’application : distribution quantique de clés (QKD)



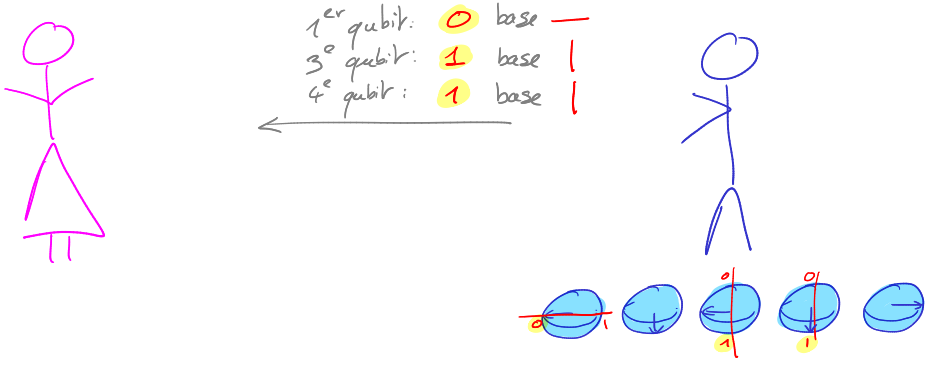
Exemple d’application : distribution quantique de clés (QKD)



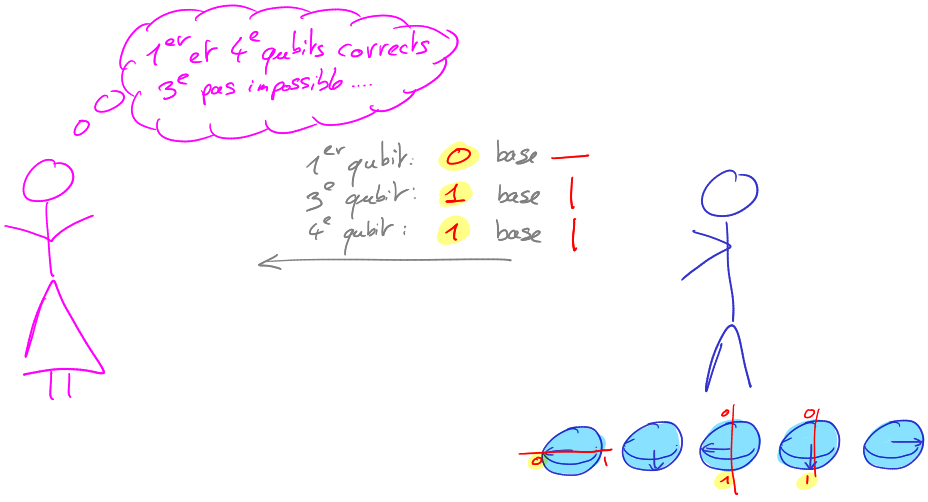
Exemple d’application : distribution quantique de clés (QKD)



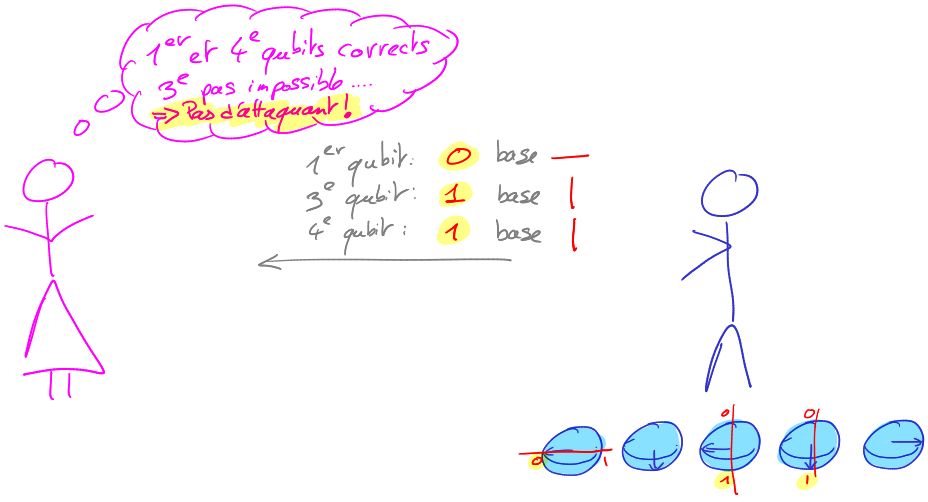
Exemple d'application : distribution quantique de clés (QKD)



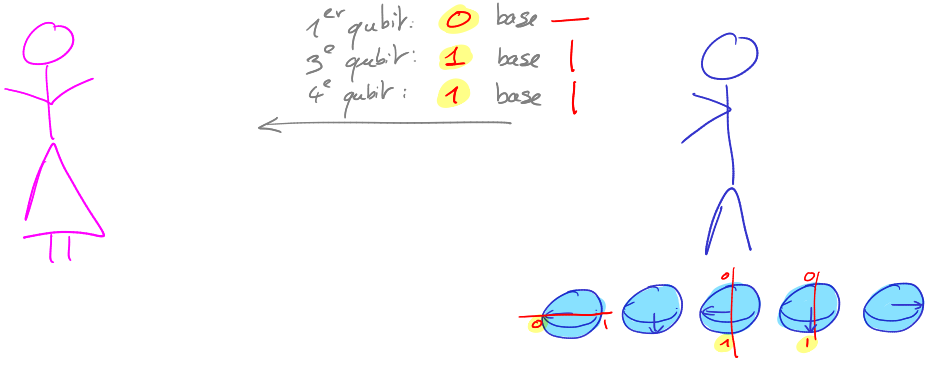
Exemple d'application : distribution quantique de clés (QKD)



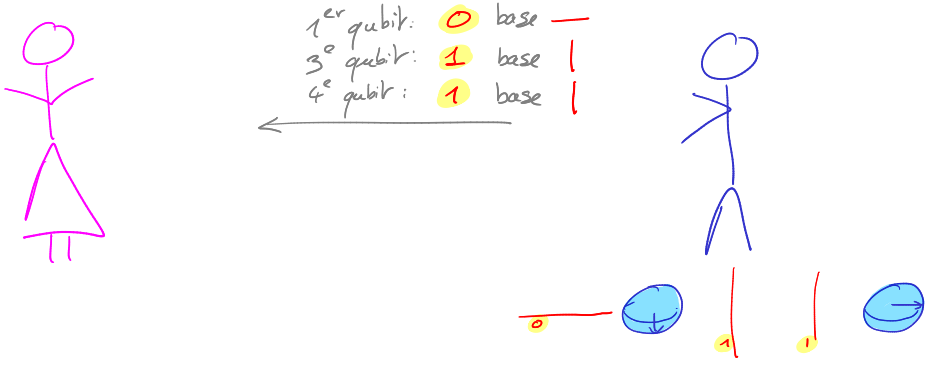
Exemple d'application : distribution quantique de clés (QKD)



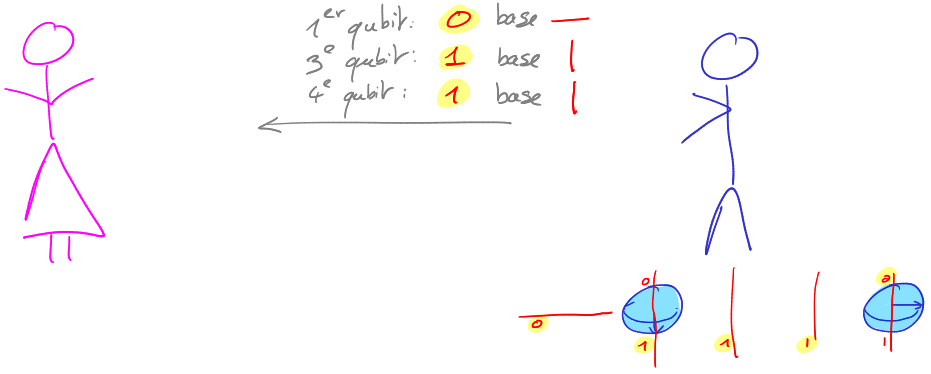
Exemple d'application : distribution quantique de clés (QKD)



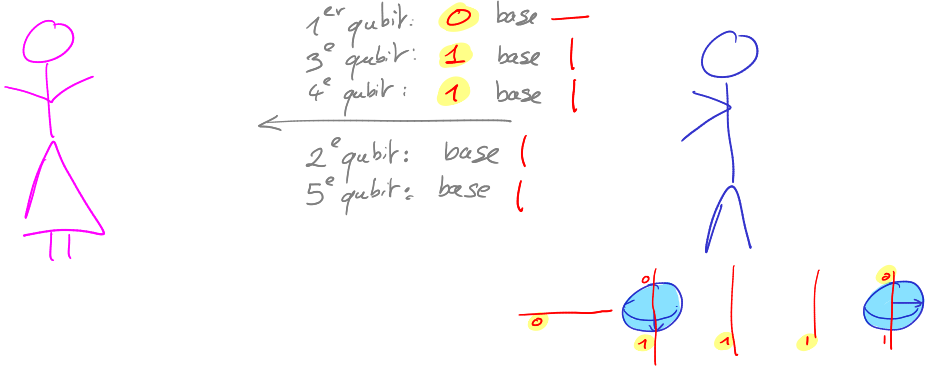
Exemple d'application : distribution quantique de clés (QKD)



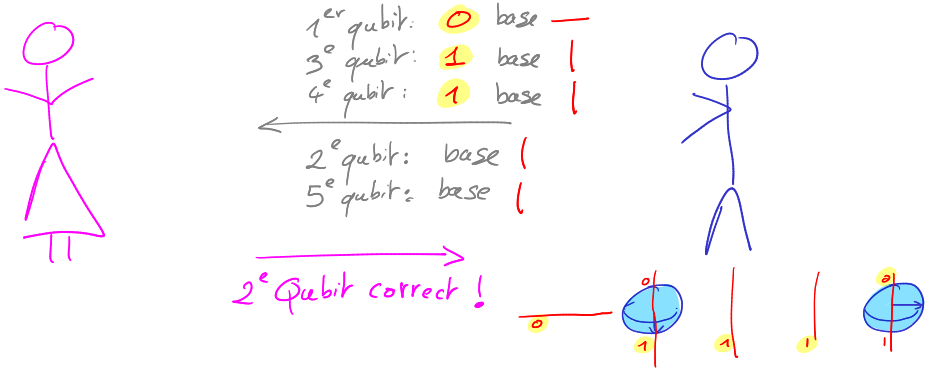
Exemple d'application : distribution quantique de clés (QKD)



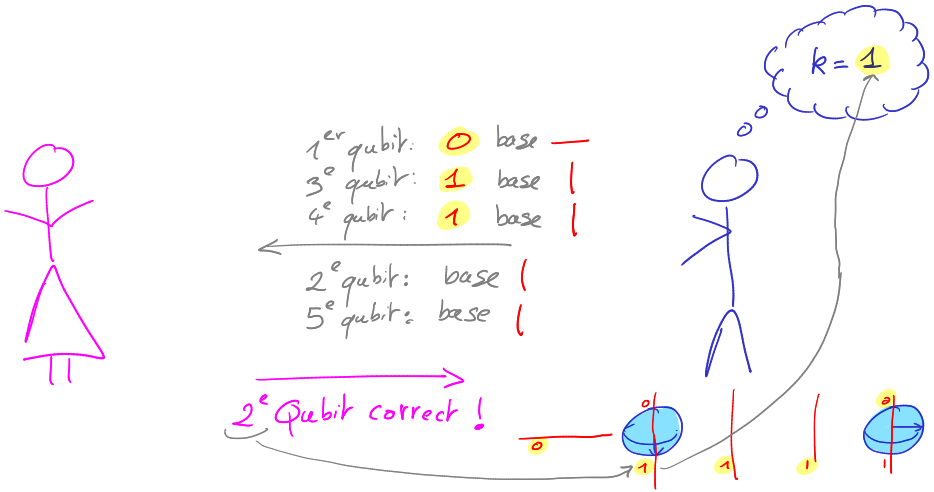
Exemple d'application : distribution quantique de clés (QKD)



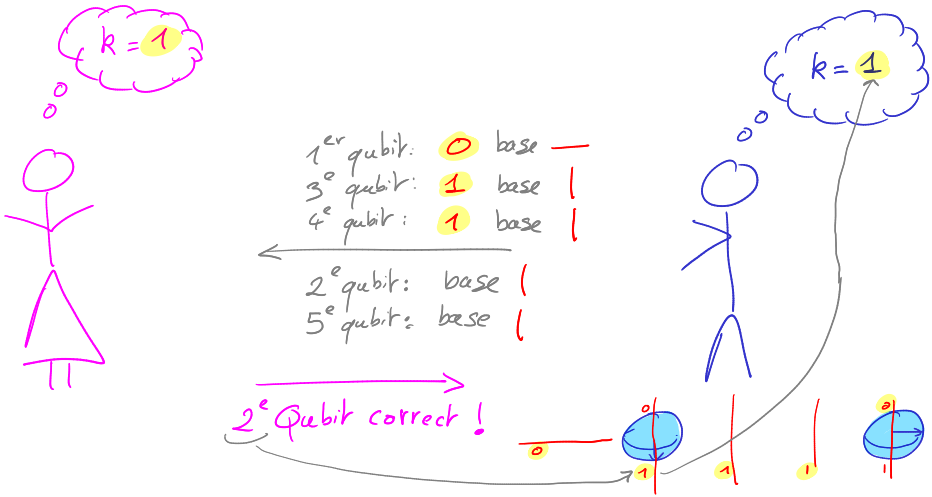
Exemple d'application : distribution quantique de clés (QKD)



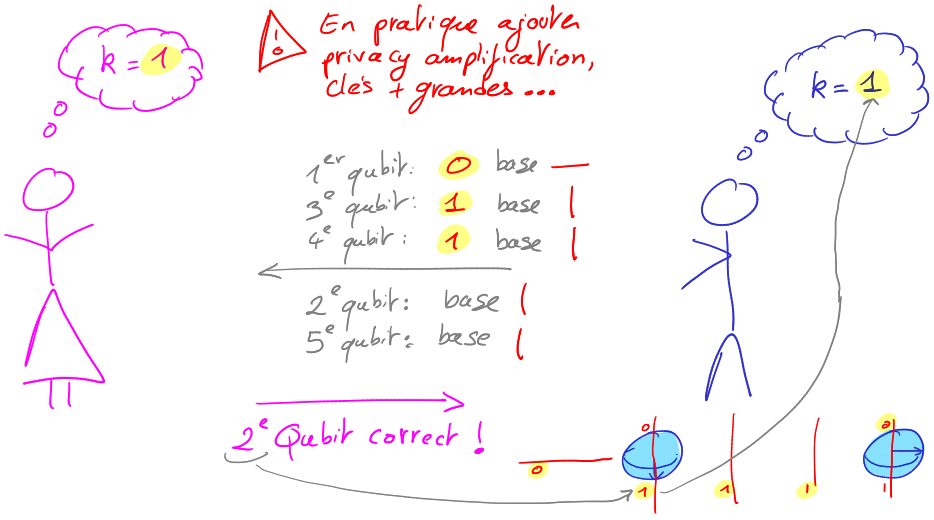
Exemple d'application : distribution quantique de clés (QKD)



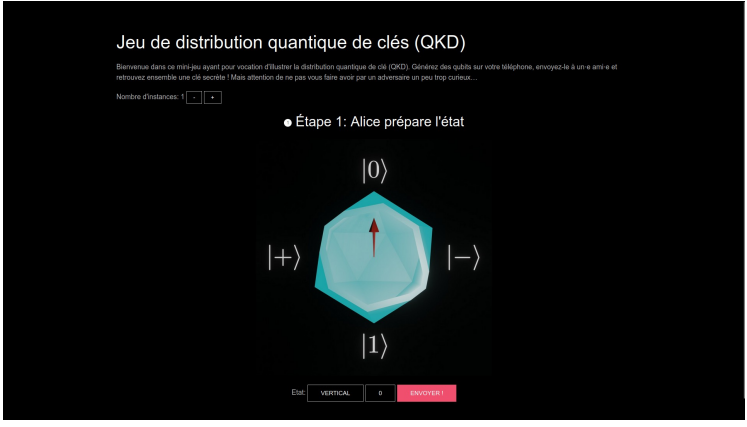
Exemple d'application : distribution quantique de clés (QKD)



Exemple d'application : distribution quantique de clés (QKD)



QKD : essayez par vous même !



https://leo-colisson.github.io/qkd-game/

Limitations QKD

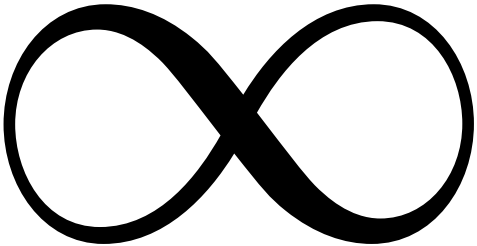
- QKD nécessite un canal **authentifié**

Limitations QKD

- QKD nécessite un canal **authentifié**
  $\Rightarrow$ nécessite signature post-quantique **seulement durant le protocole**

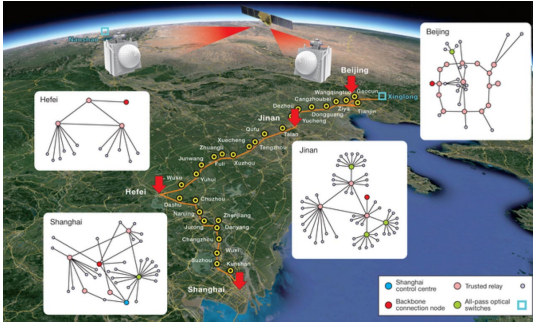
Limitations QKD

- QKD nécessite un canal **authentifié**
  $\Rightarrow$ nécessite signature post-quantique **seulement durant le protocole**
  $\Rightarrow$ même si signature cassée + tard = impossible de déchiffrer y compris avec une **puissance de calcul infinie** ! (**everlasting** security)



Limitations QKD

- Il faut un **internet quantique** (envoyer des photons uniques)
  $\Rightarrow$ via fibre faisable sur $\approx$ 100km + répéteur
  (de confiance ou nécessite mémoire quantique = dur expérimentalement)
  $\Rightarrow$ satellites = bien plus efficace



Limitations QKD

- Attention également aux attaques par canaux auxiliaires (**side-channel attacks**)

Limitations QKD

- Attention également aux attaques par canaux auxiliaires (**side-channel attacks**)
  $\Rightarrow$ protocoles **device independent** pour limiter ces attaques
  + combiner avec post-quantique

QKD en pratique

?

Quand pourra-t'on utiliser QKD ?

QKD en pratique

? Quand pourra-t'on utiliser QKD ?

⇒ **Maintenant, déjà en vente !**

QKD en pratique

? Quand pourra-t'on utiliser QKD ?

⇒ **Maintenant, déjà en vente !**

Attention : pas besoin d'un ordinateur quantique complet, mais :

- reste difficile à utiliser sur de longues distances
- potentiellement sensible aux attaques canaux auxiliaires
- faible taux de clé ≈ 500KB/h

Quantique et IA

Quantique et IA

D’innombrables manières de mélanger IA et quantique :

- Utiliser quantique pour optimiser algos/réseaux classiques :
  - Amplitude amplification/Grover/Quantum walk… : rechercher de meilleurs réseaux neuronaux etc
  - Quantum annealing : résoudre des problèmes d’optimisation
    D-Wave & NASA essayent d’optimiser des architectures de deep learning
- Utiliser classique pour essayer de prédire des processus quantiques :
  - Repliement de molécules: AlphaFold a révolutionné la chimie et la médecine (**prix nobel** 2024 de Demis Hassabis et John Jumper et David Baker)
  - Variational quantum algorithms (VQAs) : une IA classique modifie un circuit quantique

Quantique et IA

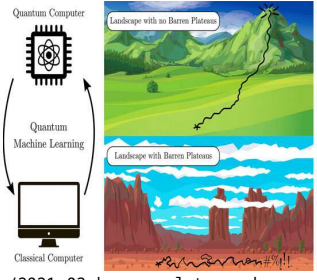
Mais **quelques réserves** :

- l'IA nécessite des expérimentations pour être vérifiée:
  $\Rightarrow$ **très difficile de tester l'IA quantique sans ordinateur quantique !!**

Quantique et IA

Mais **quelques réserves** :

- l'IA nécessite des expérimentations pour être vérifiée:
  $\Rightarrow$ **très difficile de tester l'IA quantique sans ordinateur quantique !!**
- "Barren plateau" pose souvent problème en VQA :



https://phys.org/news/2021-03-barren-plateaus-key-quantum-machine.html

Conclusion

Conclusion

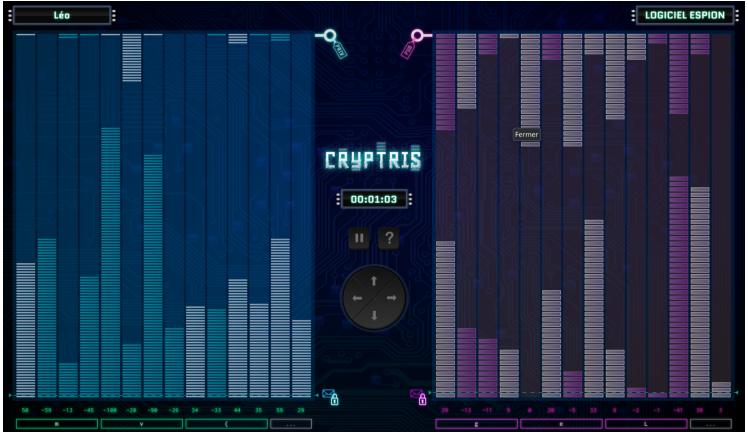
- Ordinateur quantique **casse tous les chiffrements**/signatures utilisés à l'heure actuelle sur internet
- Remplacement par **cryptographie post-quantique** (PQC, cf. standardisation NIST) d'ici 2030
- La cryptographie quantique permet d'avoir des garanties encore plus fortes (en combinaison avec PQC) = sécurité "inconditionnelle", mais encore de nombreuses difficultés pour une adoption large
- + offre de nouveaux protocoles impossibles classiquement (aléa certifié…)
- Recherche importante pour analyser les risques (crypto post-quantique vraiment sécurisée ?) et opportunités (nouveaux algorithmes…)

Aller plus loin

- Nombreux autres applications :
  - **Aléa certifié** (éviter/limiter backdoors)
    $\Rightarrow$ Magic Square
    $\Rightarrow$ déjà en vente ! `https://www.quantinuum.com/products-solutions/quantum-origin`
  - Monnaie quantique infalsifiable
  - Vérification de position, calcul délégué/multipartite…
- Device independent (DI)
- Certification de caractère quantique
- Sécurité des cryptomonnaies : signatures, mais également PoW
- Preuves de sécurité
- …

Aller plus loin : tester LWE

Pour comprendre **pourquoi LWE est difficile**, essayez de **jouer** à `https://inriamecsci.github.io/cryptris/`!




Thank you!


Thank you!